

STUDIES ON E-GOVERNANCE AND E-SECURITY: AN INDIAN PERSPECTIVE

A THESIS SUBMITTED TO

JADAVPUR UNIVERSITY

FOR

AWARD OF THE DEGREE OF

DOCTOR OF PHILOSOPHY IN ENGINEERING

IN THE FACULTY OF ENGINEERING & TECHNOLOGY
JADAVPUR UNIVERSITY, KOLKATA – 700 032, INDIA



SUBMITTED BY:

ANIL KUMAR KAUSHIK

UNDER THE SUPERVISION OF

PROFESSOR CHANDAN MAZUMDAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
JADAVPUR UNIVERSITY, KOLKATA – 700 032, INDIA

AND

DR. PARTHASARATHI BANERJEE

NATIONAL INSTITUTE OF SCIENCE, TECHNOLOGY AND
DEVELOPMENT STUDIES, CSIR, PUSA GATE, K. S. KRISHNAN MARG
NEW DELHI – 110012, INDIA

JUNE, 2012

Om Namaha Shivaya

As an arduous devotee of Lord Shiva, I make wishes and HE always blesses me with fulfillment of my wishes. This endeavour is another one in line but certainly not the last one in this journey of life.

I humbly bow down and prostrate & surrender my mind, body and soul to HIM.

(ANIL KUMAR KAUSHIK)
- a Kailasi

To my parents Late Dr. J. P. Kaushik & Mrs. S. Kaushik

प्रजासुखे सुखं राज्ञः प्रजानां हिते हितम् ।
नात्मप्रियं हितं राज्ञः प्रजानां तु प्रियं हितम् ॥

. कौटिल्यार्थशास्त्रम्-1.43

In the happiness of ruler's subjects lies his happiness; in their welfare, his welfare; whatever pleases himself he shall not consider as good, but whatever pleases his subjects he shall consider as good.

- Kautilyarthashastram – 1.43

**JADAVPUR UNIVERSITY
KOLKATA – 700 032, INDIA**

INDEX NO. 198/05/Engg.

1. **Title of the Thesis:** STUDIES ON E-GOVERNANCE AND E-SECURITY: AN INDIAN PERSPECTIVE

2. **Name, Designation & Institution of the Supervisors:**

i) Prof. Chandan Mazumdar

Department of Computer Science & Engineering,
Jadavpur University
188, Raja S. C. Mullick Road, Kolkata – 700 032
West Bengal, India

ii) Dr. Parthasarathi Banerjee

Director, National Institute of Science, Technology and Development Studies, CSIR,
Pusa Gate, K.S. Krishnan Marg,
New Delhi 110 012, India

3. **List of Publications:**

Journals

1. Mayank Vatsa, Richa Singh, P.Gupta and A.K.Kaushik, Biometric Databases, In Encyclopedia of Database Technologies and Applications by Idea Group Reference 2004
2. Overview of Biometric Technologies, In Encyclopedia of Multimedia Technology and Networking by Idea Group Reference 2004.

Conferences, Workshops, and Seminars

1. Anil K. Kaushik, Anirban Sengupta and Chandan Mazumdar, “ On the Inter-dependence of Security Controls of ISO/IEC 27002:2005”. 1st National Conference on Next Generation Computing & Information Security (NCNGCIS-2011) “Emerging Trends for Future Challenges”.25th-26th March,2011,IMS Noida.
2. P. Gupta, Hunny Mehrotra and Anil K. Kaushik, "Texture-based Iris Recognition System." Proceedings of the SPIE Symposium on Defense and Security Symposium, Orlando, USA, March 2008.
3. Anil K. Kaushik,Chandan Mazumdar, Jaya Bhattacharjee Shilpi Saha, “Model-driven Security Analysis of E-Governance Systems” egov India2007 Conference
4. Chandan Mazumdar, A.K.Kaushik and Parthasarathi Banerjee, “ On Information Security Issues in e-Governance: Developing Country View, egov India2006 Conference.

5. P. Gupta, H. Mehrotra, A. Rattani, A. Chatterjee and A.K. Kaushik, Iris Recognition using Corner Detection, Proceedings of 23rd International Biometric Conference, 16 - 21 July, 2006, Montreal, Canada.
6. Phalguni Gupta, Ajita Rattani, Hunny Mehrotra and Anil Kumar Kaushik, Multimodal Biometrics System for Efficient Human Recognition, Proceedings of SPIE 'Defense and security symposium', 9 - 13 April 2006, Florida, USA.

4. List of Patents:

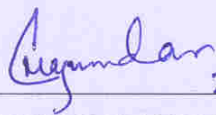
- i) NIL

5. List of Presentations in National / International Conferences:

- i) Anil K. Kaushik, Anirban Sengupta and Chandan Mazumdar, " On the Inter-dependence of Security Controls of ISO/IEC 27002:2005". 1st National Conference on Next Generation Computing & Information Security (NCNGCIS-2011) "Emerging Trends for Future Challenges".25th-26th March,2011,IMS Noida.

CERTIFICATE FROM THE SUPERVISORS

This is to certify that the thesis entitled “**STUDIES ON E-GOVERNANCE AND E-SECURITY: AN INDIAN PERSPECTIVE**” submitted by **Shri Anil Kumar Kaushik** who got his name registered on 27/06/2005 for the award of **Ph.D. (Engg.)** degree of Jadavpur University is absolutely based upon his own work done under the supervision of Prof. Chandan Mazumdar of Jadavpur University, Kolkata and Dr. Parthasarathi Banerjee of CSIR-NISTADS, and that neither his thesis nor any part of the thesis has been submitted for any degree/diploma or any other academic award anywhere before.

1.  25/6/2012
(CHANDAN MAZUMDAR)

Signature of the Supervisor
and date with Official Seal

PROFESSOR
Dept. of Computer Sci. & Engg.
JADAVPUR UNIVERSITY
Kolkata - 700 032

2. 
(PARTHASARATHI BANERJEE)

Signature of the Supervisor
and date with Official Seal

डॉ० पी० बनर्जी / Dr. P. BANERJEE
निदेशक / Director
राष्ट्रीय विज्ञान, प्रौद्योगिकी और
विकास अध्ययन संस्थान
National Institute of Science
Technology & Development Studies
पूसा, नई दिल्ली/Pusa, New Delhi-110012

ACKNOWLEDGEMENT

Successful completion of a work is often not due to inherent talent of an individual, but due to the fact that he has been supported by the persons with whom he has been associated. I would like to express my deep appreciation to several people for their whole hearted cooperation throughout my research work especially my Department, my seniors and colleagues.

I owe my profound regards to my revered supervisors, Prof. Chandan Mazumdar, Department of Computer Science & Engineering, Jadavpur University, Kolkata, India, and Dr. Parthasarathi Banerjee, Director, National Institute of Science, Technology and Development Studies, CSIR, who helped me achieve my dream by their unstinting moral and intellectual support. Both my supervisors played a fundamental role in shaping this thesis. They were extremely understanding and encouraging during the entire period of my research work.

I express my gratitude to Dr. Gulshan Rai, Director General, CERT-In & Group Coordinator (E-Security & Cyber Law), Department of Electronics & Information Technology for his continuous encouragement.

I would like to thank Prof. Aditya Bagchi, Indian Statistical Institute, Kolkata, Shri Sameer Basu, Retired Sr. Director, Deity, Shri B.J.Srinath, Sr. Director, Deity, Shri A.K.Balani, Director, Deity, Shri A.S.A.Krishnan, Sr. Director, Deity, Dr. Nageshwar Rao, Director, Deity, Shri Prafulla Kumar, Director, Deity, Dr. Yoginder Talwar, Technical Director, NIC, Deity, Shri Ashish Banati, Scientist, STQC, Deity, Prof. M Yadav, NCERT, Delhi, Prof. P.Gupta, IIT Kanpur, Dr. Richa Singh, IIIT Delhi, Dr. Mayank Vats, IIIT Delhi, Shri V.P.Sharma, Director (Academics), ICSI, Delhi, Shri Sanjay Bahl, Microsoft, Delhi, Shri S.S.Sarma, Scientist, CERT-In, Dr. Anirban Sengupta, Research Scientist, Jadavpur University, Mrs. Jaya Bhattacharjee, Research Scientist, Jadavpur University, and all members of the Centre for Distributed Computing, Jadavpur University (CDC-JU) for their whole hearted support in every step during my work. I am extremely grateful to the Department of Electronics & Information Technology, Govt. of India for providing me opportunity to carry out this research.

I express my heartfelt gratitude to all my teachers who have guided me during my formative years. I can never forget the contribution of my mentors and friends; they helped me during my

school days and onward life in every way possible and inspired me to take up research work later in life.

I wish to thank my wife Dr. Pankaja Ghai Kaushik, my daughter Priyamvada and family members for putting up with me while I spent most of my late evenings in research work. The patience and consideration they have shown have been beyond measure.

Last, but not the least, I would like to acknowledge the contribution of my father, Late Dr. J.P.Kaushik, who taught me never to give up in times of adversity, and my mother Smt. S. Kaushik, who has always stood by me through thick and thin.

Finally, a big “THANK YOU” to all my friends, colleagues, and well-wishers who have always supported me and continue to do so in all my endeavors. This effort would not have bore fruit without help from everyone of you.

ANIL KUMAR KAUSHIK

ABSTRACT

Governance relates to the management of all such processes that, in any society, define the environment which permits and enables individuals to raise their capability levels, on one hand, and provide opportunities to realize their potential and enlarge the set of available choices, on the other. These processes, covering the political, social and economic aspects of life impact every level of human enterprise, be it the individual, the household, the village, the region or the nation.

Electronic-Governance (e-Governance) is fast emerging as an important tool for achieving good governance especially with regard to improving efficiency, transparency and making interface with government user-friendly. Major types of e-government services are **Government-to-Citizen (G2C)**, **Government-to-Business (G2B)**, and **Government-to-Government (G2G)**. e-Governance Service Delivery Gateway is one way governments attempt to deliver services directly to the citizen, without the citizen having to go to a government building. It provides seamless interoperability and exchange of data across heterogeneous applications of geographically dispersed departments. This was proposed by the National e-Governance Plan (NeGP) that was approved by the Government of India in the month of May 2006. It consists of a National Service Delivery Gateway, State Service Delivery Gateways, and Data Centres.

E-governance applications handle sensitive data of the government and public. The security requirements of the data are different for different applications. The security parameters to be considered are: Confidentiality, Integrity, Availability, Authentication, and Non-Repudiation.

There should be appropriate mechanisms for identification and authentication of general citizens before they are allowed access to e-services. The Unique Identification Authority of India (UIDAI) has been created with the mandate of providing a Unique Identity (Aadhaar) to all residents of India. The UIDAI proposes to provide online authentication using demographic and biometric data. The UID (Aadhaar) Number, which uniquely identifies a resident, will give individuals the means to clearly establish their identity to public and private agencies across the country.

This thesis discusses various aspects of e-governance and suggests means to ensure that electronic services are delivered securely.

Dissemination of Work

Journals

1. Mayank Vatsa, Richa Singh, P.Gupta and A.K.Kaushik, “Biometric Databases”, In Encyclopedia of Database Technologies and Applications by Idea Group Reference 2004
2. Mayank Vatsa, Richa Singh, P.Gupta and A.K.Kaushik, “Overview of Biometric Technologies”, In Encyclopedia of Multimedia Technology and Networking by Idea Group Reference 2004.

Conferences, Workshops, and Seminars

1. Anil K. Kaushik, Anirban Sengupta and Chandan Mazumdar, “On the Interdependence of Security Controls of ISO/IEC 27002:2005”. 1st National Conference on Next Generation Computing & Information Security (NCNGCIS-2011) “Emerging Trends for Future Challenges”. 25th-26th March, 2011, IMS Noida.
2. P. Gupta, Hunny Mehrotra and Anil K. Kaushik, “Texture-based Iris Recognition System”. Proceedings of the SPIE Symposium on Defense and Security Symposium, Orlando, USA, March 2008.
3. Anil K. Kaushik, Chandan Mazumdar, Jaya Bhattacharjee Shilpi Saha, “Model-driven Security Analysis of E-Governance Systems” egov India2007 Conference.
4. Chandan Mazumdar, A.K.Kaushik and Parthasarathi Banerjee, “On Information Security Issues in e-Governance: Developing Country View, egov India2006 Conference.
5. P. Gupta, H. Mehrotra, A. Rattani, A. Chatterjee and A.K. Kaushik, “Iris Recognition using Corner Detection”, Proceedings of 23rd International Biometric Conference, 16 - 21 July, 2006, Montreal, Canada.
6. Phalguni Gupta, Ajita Rattani, Hunny Mehrotra and Anil Kumar Kaushik, “Multimodal Biometrics System for Efficient Human Recognition”, Proceedings of SPIE ‘Defense and security symposium’, 9 - 13 April 2006, Florida, USA.
7. Anil Kumar Kaushik, Anirban Sengupta, Chandan Mazumdar and Parthasarathi Banerjee, “Information Security Issues of e-Service Delivery Gateways”, communicated.

TABLE OF CONTENTS

	Page No.
Acknowledgement	i
Abstract	iii
Table of Contents	iv
List of Figures	vii
List of Tables	viii

CHAPTERS

1. Introduction	1
1.1 Prologue	1
1.2 Electronic Governance	2
1.3 Common interactions in e-Governance	3
1.4 Stages of e-Governance	5
1.5 Relation with Enterprise Information Security	6
1.6 Motivation	7
1.7 Objectives	8
1.8 Organisation of the Thesis	8
 2. Origin and History of Governance	 9
2.1 Introduction	9
2.2 The Concept of Governance	9
2.3 A Brief History of Governance	10
2.4 Summary	28
 3. Evolution of e-Governance	 30
3.1. Introduction	30
3.2 Use of ICT in Governance	31
3.3 Concept of e-Governance	33
3.4 e-Governance Models	40

3.5	Challenges of e-Governance	46
3.6	Initiatives of the Government of India	51
3.7	Summary	52
4.	e-Governance Security Requirements	54
4.1	Introduction	54
4.2	Security Controls	56
4.3	Security Classification for Information	58
4.4	Information Security Threats and Security Requirements	58
4.5	Security Postures to Support Data Characteristics and Access	64
4.6	A Structured Approach to Information Security Design	79
4.7	Summary	82
5.	Security of On-line Government Service Delivery	83
5.1	Introduction	83
5.2	Online Government Services	83
5.3	Integration of Services- Concept of Service Delivery Gateway	85
5.4	Architecture and Implementation of SSDG and NSDG	93
5.5	Requirements to Ensure Secure Service Delivery	99
5.6	Security Controls for Delivery Gateways	105
5.7	Assuring Secure Service Delivery	106
5.8	Summary	107
6.	Unique ID and Online Service Delivery – A Policy Perspective	109
6.1	Introduction	109
6.2	Requirements of Identification and Authentication of General Citizen	109
6.3	Role of Biometrics in I&A of Citizens	111
6.4	Unique ID Card System as Vehicle for Biometric I&A	114
6.5	Security Issues of Unique ID Card System	123
6.6	The Policy Perspective	125
6.7	Summary	129

7. Conclusion and Future Work	131
7.1. Summary of Contributions	131
7.2. Scope of Improvement	132
7.3. Future Work	132
 Annexure – I: Timeline of Evolution of Governance	 134
Dissemination of Work	136
Bibliography	137

LIST OF FIGURES

Figure No.	Figure Title	Page No.
3.1	Key Components of Government ICT	31
3.2	Advantages of e-Governance	38
3.3	Interactions between main groups in e-Governance	40
4.1	Defense-in-depth	57
4.2 (a)	Indian websites defaced during 2006 and 2007, respectively	61
4.2 (b)	Indian websites defaced during 2008 and 2009, respectively	61
4.2 (c)	Indian websites defaced during 2010	61
4.2 (d)	Indian websites defaced during 2011	62
4.3	CIA Triad	65
5.1	e-Governance Service Delivery framework	91
5.2	Conceptual Gateway Cluster	93
5.3	Gateway infrastructure operating at the Centre and States in e-Governance service delivery	94
5.4	Positioning NSDG in various e-Governance Projects	96
6.1	ASA Server Architecture	116
6.2	Policy Hierarchy	126

LIST OF TABLES

Table No.	Table Title	Page No.
3.1	Main group interactions in e-Governance	40
3.2	e-Governance Maturity Model (Gartner)	42
3.3	Examples of Government Information	43
3.4	Overview of e-Governance solutions for each phase	44
4.1	Security requirements of Broadcasting model	67
4.2	Security requirements of Critical Flow model	68
4.3	Security requirements of Comparative Analysis model	70
4.4	Security requirements of E-Advocacy model	72
4.5	Security requirements of Interactive Service model	73
4.6	Access requirements of Users for Broadcasting model	77
4.7	Access requirements of Users for Critical Flow model	78
4.8	Access requirements of Users for Comparative Analysis model	78
4.9	Access requirements of Users for E-Advocacy model	78
4.10	Access requirements of Users for Interactive Service model	78
5.1	Services to be implemented through SSDG	88
5.2	Services to be implemented through NSDG	92
5.3	Risks: User Perspective	101
5.4	Risks: Service Owner Perspective	103

5.5	Risks: Service Supplier Perspective	104
5.6	Security Control Classes and Families	105
6.1	Properties of Biometric Factors	114
6.2	Attributes for Aadhaar Authentication	122

Introduction

1.1 Prologue

The issue of governance has, in recent times, emerged at the forefront of the development agenda for any government. Good governance is one of the most crucial factors required if targets of the government are to be achieved. It is also this factor, or rather lack of it, which could be the cause of immense disappointment and missed development opportunities.

Governance relates to the management of all such processes that, in any society, define the environment which permits and enables individuals to raise their capability levels, on one hand, and provide opportunities to realize their potential and enlarge the set of available choices, on the other. These processes, covering the political, social and economic aspects of life impact every level of human enterprise, be it the individual, the household, the village, the region or the nation. It covers the State, civil society and the market, each of which is critical for sustaining human development. The State is responsible for creating a conducive political, legal and economic environment for building individual capabilities and encouraging private initiative. The market is expected to create opportunities for people. Civil society facilitates the mobilization of public opinion and peoples' participation in economic, social and political activities.

The universally accepted features of good governance are exercise of legitimate political power, and formulation and implementation of policies and programmes that are equitable, transparent, non-discriminatory, socially sensitive, participatory, and above all accountable to people at large. There could however be aspects of governance that are contextually driven and geared to address local concerns.

Experience shows that while good governance can help secure human well being and sustained development, it is equally important to recognize that poor governance could well erode individual capabilities, as well as institutional and community capacities to meet the needs of sustenance.

1.2 Electronic Governance

Electronic-governance (e-Governance) [31, 62, 63, 80] is fast emerging as an important tool for achieving good governance especially with regard to improving efficiency, transparency and making interface with government user-friendly. So far the emphasis has been on providing connectivity, networking, technology upgrade, selective delivery systems for information and services, and a package of software solutions.

Unprecedented growth of innovative services and technologies are challenging the demarcation of various services, service providers, users and government regulations in Information and Communication Technology (ICT) industry. The success of the convergence regime would lie in ensuring a seamless transition to the new services and information delivery systems.

The delivery of government services has become very inefficient because of too much discretion at every level, lack of transparency and cumbersome record management.

Electronic Governance can be defined as the application of ICT to the processes of Government functioning in order to bring about Simple, Moral, Accountable, Responsive and Transparent (SMART) Governance. Electronic governance also involves transformation from being a passive information and service provider to active citizen involvement. Evolution of e-Governance is a highly complex process requiring provision of hardware, software, networking and re-engineering of the procedures for better delivery of services.

Traditionally, interactions between a citizen or business and government agency took place in a government office. With emerging ICT it is possible to locate service centers closer to clients. e-Governance is an opportunity to take advantage of the increased productivity and reduced costs that can be achieved using Internet-based technologies. Even better, e-Governance can enhance citizen's access to government information and services (both central and local), and can provide new ways to increase citizen participation in the democratic process.

e-Governance may include a broad range of services for almost all segments of society. The most common areas of e-Governance applications are:

- Agriculture
- Digital democracy

- Education
- Electronic commerce and business regulations
- Health
- Law enforcement and courts
- Taxation and revenue
- Transport

The benefits of e-Governance are as follows:

- The citizen benefits because there is transparency, efficiency and integrity in his dealings with the government; furthermore, there is easy access to information.
- The government benefits because it reduces redundancy and duplication. The processes of data collection, analysis and audit are made easier. Decision making gets expedited. And there can be tremendous improvements in specialized areas such as criminal justice, transport etc.
- The business community benefits because e-Governance can become a catalyst and a channel for e-business, and in fact it has been so in places like the USA, UK, Canada, Australia and Singapore. Furthermore a web-based government will enable payment of taxes online, and reduce corruption and manipulation.

1.3 Common interactions in e-Governance

e-Governance services focus on four main stakeholders: citizens, the business community, government employees, and government agencies. e-Governance aims to make interaction with citizens, businesses, government employees, government agencies and other governments more convenient, friendly, transparent, inexpensive and effective. In an e-Governance system, individuals are able to initiate a request for a particular government service and then receive that government service through the Internet or some computerized mechanism. In some cases, the government service is delivered through one government office, instead of many. In other cases, a government transaction is completed without direct in-person contact with a government employee.

The four types of e-Governance services [9, 14] are **Government-to-Government (G2G)**, **Government-to-Business (G2B)**, **Government-to-Citizen (G2C)** and **Government-to-Employee (G2E)**.

G2G services take place at two levels: at the local or domestic level and at the international level. G2G services are transactions between the central/national and local governments, and between department-level and attached agencies and bureaus. At the same time, G2G services are transactions between governments, and can be used as an instrument of international relations and diplomacy.

G2B transactions include various services exchanged between government and the business community, including dissemination of policies, memos, rules and regulations. Business services offered include obtaining current business information, downloading application forms, renewing licenses, registering businesses, obtaining permits, and payment of taxes. The services offered through G2B transactions also assist in business development, specifically the development of small and medium enterprises. Simplifying application procedures that would facilitate the approval process for SME (Small and Medium Enterprises) requests would encourage business development.

On a higher level, G2B services include e-procurement, an online government-supplier exchange for the purchase of goods and services by government. Typically, e-procurement websites allow qualified and registered users to look for buyers or sellers of goods and services. Depending on the approach, buyers or sellers may specify prices or invite bids. E-Procurement makes the bidding process transparent and enables smaller businesses to bid for big government procurement projects. The system also helps government generate bigger savings, as costs from middlemen are shaved off and purchasing agents' overhead is reduced.

G2C includes information dissemination to the public, basic citizen services such as license renewals, ordering of birth/death/marriage certificates and filing of income taxes, as well as citizen assistance for such basic services as education, health care, hospital information, libraries, and the like.

G2E services encompass G2C services as well as specialized services that cover only government employees, such as the provision of human resource training and development that improve the bureaucracy's day-to-day functions and dealings with citizens.

1.4 Stages of e-Governance

There are four general stages of e-Governance, which in most cases must follow a particular order.

Stage 1: Information Technology Frameworks

Deployment of a basic Information Technology framework is a pre-requisite for any foray into e-Governance. This includes the following:

- a) Computers in some minimum number and with some minimum capability;
- b) Interconnectivity of those computers (networking);
- c) Basic bandwidth for applications like internet access and email; and
- d) A communication platform – such as an intranet.

The development of an Intranet for employees and constituents of a Government agency for centralized access to collaborative work tools and information will dramatically increase efficiency by creating a tap on common knowledge pool as well as providing productivity tools. The choice of computers is relatively easy; however, the software is more critical a component than the hardware. The price of a PC is pushed up by the cost of license for commercial software. Open Source software, which is available without fee for license, may be used.

Stage 2: Digitization

Once technology has been deployed and a network put in place, the next step is to make sure that all content and processes of the administration is digitized. Processes and systems should ensure that digitization and tagging of documents becomes a habit, not one isolated project. Digitization and tagging ensures that time is saved in mundane tasks like locating files. If the digitization process does not take place, the purpose of implementing e-Governance is defeated. One cannot imagine providing better services to citizens unless the department is internally equipped to provide those services.

Stage 3: Citizens Access

Once the digitization process is in place, the next logical step for an administration is to make the information available to citizens. One way of doing this is through a ‘Citizens’ Portal’. This essentially involves transforming the information produced by the Government to make it interactive, attractive and user-friendly, and then allowing it to be accessed by citizens. This can

change the experience that citizens have with the administration and also increase the productivity of the officers by saving their time from routine requirements of the general public.

Stage 4: Content

Even though Governments are one of the richest sources of information, the content generated by the government fails to involve citizens. This is very dangerous because ultimately, after all the computers and networks and state wide fibre optic connections are ready, the content that flows through those networks will ensure the success or failure of e-Governance. Managing this last link to the citizen is a challenge and unfortunately, has been one in which Government around the world have been singularly unsuccessful.

1.5 Relation with Enterprise Information Security

The e-Governance structure using ICT pushes the government institutions more towards an enterprise, comprising of People, Process and Technology. It can be viewed as a collection of assets and their interrelationship. As such, the e-Governance system is very similar to the multi-tier IT systems having back-end data store, the business logic, the information delivery system and the user interface sub-systems. These assets contain vulnerabilities which may be exploited by threats to breach information security of enterprises. In order to achieve SMART governance, the urgent need is to secure the data and the transactions at each level of the e-Governance system, including the infrastructure security.

While the security of e-Governance infrastructure is largely the responsibility of the relevant Dept. of Home Affairs, the security of data and IT infrastructure can take a lot of imports from the enterprise level information security. There are a number of very good standards like ISO 27000 series, COBIT, and BIS (the German Standard) in information security. These standards are based on the best practices of Information Security followed in the industry. However, there are no such international standards specifically for the e-Governance security, apparently because each country has its own method, culture and legacy of governance. As such, the information security of governance systems should be in line with the e-Governance approach of a specific nation state. Also, it may be noted that many of the methods and controls of enterprise information security can be adapted to the e-Governance system as well.

This observation led to this study of e-Governance and E-security from an Indian perspective.

1.6 Motivation

In a country like India, the mind-boggling number of citizens and the variety in geography, language, culture, and ethical standards make it difficult to deliver good governance. Of particular importance are the issues of speedy, transparent and accountable governance. As such, the Government of India, from the very initial stages, has constituted the Department of Administrative Reforms and Public Grievances for continuous evaluation and upgradation of Governance Structures, Technologies and Procedures. In the last decade, with the advent of Internet, the government introduced the ambitious National e-Governance Plan [57], with the vision:

“Make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realise the basic needs of the common man”.

Since then, the Govt. of India is continuously introducing various changes in governance mechanisms and technologies for e-Governance. This started with the introduction of various government web-sites, introducing G2G and G2B services, setting of State-level Wide Area Networks (SWAN), State Data Centres, Common Service Centres and finally the very recent Service Delivery Gateways. The other most ambitious initiative is the UIDAI project to provide the citizens with the Unique ID Card for Identification and Authentication required for facilitating smooth e-service delivery to the citizens.

These initiatives require huge investments and drastic changes in the way government services are delivered to the citizens. Also, since these initiatives are going to cover all the citizens of the country, the amount and sensitivity of the data stored and handled are also huge.

It is true, the government has taken some initiatives for ensuring security of the data and services delivered to the citizens. But it requires serious academic approach for the analysis and appraisal of the e-Governance system security with a focus on Indian perspective for the successful implementation and maintenance of such systems [81]. Such a study is important from the point of view of the general citizens as well as the government. The academic challenges of such a study include the historical development of governance on one hand and the information security aspects on the other. This triggered the motivation of the present dissertation.

1.7 Objectives

Objectives of the dissertation were:

- (a) To study the inception and historical development of governance, with a focus on the Indian sub-continent.
- (b) To study the evolution of e-Governance
- (c) To analyze the IT security vulnerabilities and controls for the e-Governance system and their relationship to the enterprise security standards
- (d) To analyze the IT security approaches for the National and State level Service Delivery Gateways
- (e) To analyze the IT security issues of the UIDAI system.

1.8 Organization of the Thesis

Rest of the thesis is organized as follows.

Chapter 2 discusses in a brief manner the history and development of Governance. In Chapter 3, a brief account of the evolution of e-Governance and its various models is presented. Chapter 4 presents a detailed findings of the Information Security requirements of e-Governance. In Chapter 5, the architecture and implementation aspects of the National and State level e-Service Delivery Gateways have been presented along with a discussion on the IT Security aspects of the systems. Chapter 6 presents the proposed Unique ID System architecture and the issues related to the privacy and security of the data stored and transacted in the UIDAI project. Finally, in Chapter 7, the summary of contributions of this dissertation is presented along with the proposed extensions of this work.

Origin and History of Governance

2.1 Introduction

In this chapter we introduce the concept of Governance and touch upon the historical aspects of Governance. It basically covers the meaning of the word Governance, a brief of governance with reference to European countries and Ancient Indian perspective particularly from epic age to modern time.

2.2 The Concept of Governance

With the beginning of civilization, there arose a need for smooth administration and division of responsibilities. Since the population started to increase, people grew concerned about their welfare and able ruling. This led to the rise of an organizational structure which dealt with the nuances of firm ruling and governance. According to the American Heritage Dictionary governance is defined as “the act, process or power of governing government”; the Oxford English Dictionary defined the governance as “the act or manner of governing, of exercising control or authority over the actions of subjects; a system of regulations”.

According to The International Encyclopedia of the Social Sciences, **Governance** is the act of governing. It relates to decisions that define *expectations*, grant power, or verify performance. It consists of either a separate process or part of management or leadership processes. A government typically administers these processes and systems.

In the case of a business or of a non-profit organisation, governance relates to consistent management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility. For example, managing at a corporate level might involve evolving policies on privacy, on internal investment, and on the use of data.

To distinguish the term governance from government; “governance” is what a “government” does. It might be a geo-political government (nation-state), a corporate government (business entity), a socio-political government (tribe, family etc.), or any number of different kinds of government, but governance is the actual exercise of management power and policy, while

government is the instrument (usually collective) that does it. The term government is also used more abstractly as a synonym for governance.

Perhaps the widest definition of governance is given in the Report of the Commission on Global Governance i.e. “Our Global Neighbourhood”. According to this report, “Governance is the sum of the many ways individuals and institutions, public and private, manage their common affairs. It is a continuing process through which the conflicting or diverse interests may be accommodated and co-operative action may be taken. It thus includes formal institutions and regimes empowered to enforce compliance, as well as informal arrangements that people and institutions either have agreed to or perceive to be in their interest”.

The universally accepted features of good governance basically include the exercise of legitimate political power, formulation and implementation of policies and programmes which are equitable, transparent, non-discriminatory, socially sensitive, participatory, and above all accountable to the people at large. However, there could be aspects of governance which are contextually driven and geared to address the local concerns.

In this discourse, we consider that there is a body, nominated, selected or elected, which executes the actions of governance and the citizens expect and get the services from the body for their benefit, possibly by paying taxes and service charges.

2.3 A brief History of Governance

In this section a brief review of literature on the history of is presented. The focus will be on Ancient Greek History and the Indian perspective. The Indian Perspective is discussed in the light of the Ancient, Medieval, British Raj and Post-independence India. A brief timeline of governance starting from Indus Valley Civilization to Independence of India has been presented in Annexure – I.

2.3.1 Governance in Europe

The era of Ancient Greece spread over 1100 BC to around 146 BC and was made up of several city-states or “polis”, the most prominent of which was Athens. The population of Ancient Greece consisted of free citizens and slaves. Women took their place in society through their husbands. The free citizens were primarily farmers and military service was compulsory.

Principles of governance in ancient Greece evolved from being a government of landowners, then a council of free citizens, and finally to being a democracy.

The emergence of political systems during the Archaic period [64] led to different forms of governance among the many city states in Ancient Greece during the Archaic period, 750-500 BCE [27]. Because the Greek city-states were self-governing entities and not bound together by any type of central control or an empire, different governing formats developed independently and allowed for experimentation and change.

One-man rule known as basileus with religious connotations was transformed into Tyranny in order to thwart attempts by the aristocrats in forming an oligarchy. Pheidon of Argos and Draco of Athens were notable amongst such rulers.

Democracy refers to the power (kratos) of the people (demos). In Athens, however, only 10% of the people were considered citizens and able to participate fully in the political structure. Participation was based on land ownership (property) which opened up the democratic form to charges of elitism. As a result of Solon's reforms, the Ekklesia or Assembly was open to all adult male citizens. Athenian democracy, unlike today, was direct democracy.

Some city-states favoured monarchy. Sparta actually had two kings that acted as a check against each other (perhaps like the system of Consuls in the Roman Senate). Sparta also featured a people's Assembly, the Appella or Demos, which met once a month. Participation was limited to male citizens thirty years of age and older. The Appella voiced, quite literally, the judgment of the people.

Oligarchies represented another form of government where in some city-states, governance rested with an elite group of men, an aristocratic committee of wealthy community leaders that facilitated daily government. The term oligarchies refers to rule by the "few" (oligoi). Their members considered themselves the "best men," a term from which "aristocrat" is derived. Government functions were basically divided, in terms of individual responsibilities.

Many city-states also had chief administrators. In Athens, these were known as archons, while in Sparta an Ephor was part of a five-man committee with extensive executive responsibilities. These top magistrates might be compared to modern "city managers."

Although the general definitions of Greek government appear simplistic but it was exceedingly complex because of it varied and changed between the city-states, Athens, for

example, went through various incarnations of government and only attained the height of direct democracy under Pericles. The attempt to perfect government was best expressed by Aristotle, who compiled and analyzed many of the city-state constitutions in order to develop one most representative of political ideals dear to the citizens.

Modern governmental structures and institutions may be the product of many influences over time. Yet the contributions of early Greek governmental systems stand out as the first expressions of participation in political systems by ordinary people, *albeit* male citizens.

2.3.2 The Ancient Indian Perspective

Indian subcontinent has a rich historical and cultural legacy with the earliest civilisations along with Mesopotamia, Egypt and China. India was invaded many times by foreign rulers and has preserved its cultural heritage.

The word “governance” has been used with different meanings in different parts of India during different times. Ancient India had seen many forms of governance and government during different periods in the region. Even within a given territory there were many kingdoms with different ways of governance [67].

Archaeological excavations and research have reveal that a highly developed urban civilization in ancient India, which stretched across approximately 1520 kilometres, extending from the area on the upper Sutlaj in contemporary Punjab to Lothal in Gujarat. Historians are of the view that this civilization flourished in the third millennium before the birth of Christ. The Harappa and Mohanjodaro perhaps had democratic government setup with no evidence of monarchy being found.

The rudimentary administrative system headed by tribal chieftains was transformed by a number of regional republics or hereditary monarchies that devised ways to appropriate revenue and to conscript labour for expanding the areas of settlement and agriculture farther east and south, beyond the Narmada River. These emergent state governments collected revenue through officials, maintained armies, and built new cities and roads. By 600 B.C., sixteen such territorial powers--including the Magadha, Kosala, Kuru, and Gandhara--stretched across the North Indian plains from modern-day Afghanistan to Bangladesh.

While there are different sources which can be accessed for understanding the concept of Governance, we limit our review, in the interest of brevity but without compromising on

relevance and import, to two key authorities: the Rig Veda and the epic, Mahabharat. We supplement these with the prescriptions of Manu Smriti and the later day political treatise, the Artha Sastra of Kautilya, and the great Tamil classic, Thiru Kural, by Thiru Valluvar [76].

Rig Veda [10]

The Rig Veda leaves no one in doubt that the king was “no longer merely a leader of a primitive tribe, but occupied a position of pre-eminence which was deliberately distinguished in all possible ways from the rest of the people.” Two assemblies called sabha and samiti formed an essential feature of government. Sabha denotes both “the people in conclave” and the “hall” which was the venue of their meeting. The Samiti was “a more comprehensive conference including not only the common people but also Brahmanas [read, learned men and women] and rich patrons”. Thus, it would appear that the Samiti was an august assembly of a larger group of the people for the discharge of tribal (or political) business and was presided over by the king. The Sabha, on the other hand, was “a more select body, was less popular and political in character than the Samiti”, and together these two bodies “acted as healthy checks on the power of the king”. It is interesting to note that despite these built-in checks and balances on the abuse of power by the king, the two bodies were exhorted to be united in their approach, speaking together and being all of one accord. Clearly, this was an open exhortation to the two consultative and countervailing bodies to discuss, debate and to arrive at a consensus of counsel to the king. There was yet another institution that the Rig Veda alludes to in the context of curbing any abuse of power by the king, viz, the unique position of the purohita. His status is quite high, his counsel is respectfully listened to and obeyed, and never ever disregarded; a king with such wise counsel is assured of success in wars and obeisance from people in his kingdom and elsewhere.

Dharmashastra

While reviewing the History of Governance we come across with Dharmashastra texts [50], which are of great source of information regarding ancient Indian system of governance. Dharmashastra text describes the code of conduct for human kind. These codes are preserved primarily in “sutras” and “smritis” which are compiled in different time periods. Grihyasutras, Dharmasutras, Smritis and Arthashastra contains the material of Dharmashastra which are authored by various Dharmashastra scholars i.e. Apastamba, Gautam, Vishnu, Manu, Yajnyavalkya, Parashar, Brihaspati, Narad, Katyayan etc. Dharmashastra texts focus on three major topics aachar, vyavahar and prayashchitta:

- (i) Aachar, rules are pertaining to daily rituals, life-cycle and other duties of four castes or varnas,

- (ii) Vyayahar, rules are pertaining to the procedures for resolving doubts about dharma and rules of substantive law categorized according to the standard eighteen titles of Hindu law and
- (iii) Prayascitta, rules are about expiation and penances for violations of rules of dharma

To ascertain the principles regarding governance in ancient India, we need to look into vyahavaar portion of Dharmashastra texts. For governance or issues pertaining governance, “Rajdharm”, “Nitishashtra”, “Rajshastra” and “Dandaniti” terms have been used by the various authors of Dharmashastra. According to the Shantiparvan originally in the krita age, there was no king or shashak. Then delusion, greed and lust entered and started destroying the Dharma. In order to provide protection against the complete destruction of Dharma, Brahama composed a beautiful work called Dharmashastra. For securing social code of conduct, requirement of government was felt inevitable. Some centuries before and after the Christian era, monarchy alone is generally envisaged by ancient Indian political thinkers. The result has been that the King came in practice to be almost synonymous with government in monarchical system of governance. All the Dharmashastra texts present monarchical system of governance. For the stability and welfare of good governance, Dharmashastra texts suggest seven tools which are known as seven angas of state which are as follows :

- (i) Swamin (ruler or sovereign)
- (ii) Amatyas (minister)
- (iii) Janapada (The territory and people)
- (iv) Durga (Fortified city or capital)
- (v) Kosha (Tresury or accumulated wealth)
- (vi) Danda (Army or Force)
- (vii) Mitra (Allies)

All these are most essential elements for establishing good governance of any state. The most essential elements were not only known to ancient authors of Dharmashastra but also they had given a great importance to these elements and therefore, all seven tools have been elaborated in detail in all Dharmashastra texts.

Dharmashastra authors were well aware of significance of law and order, so, they had given their thought to administer justice impartially and to punish the guilty. Providing justice was considered as one of the prime function of the ruler in any set of governance during that era. In the exercise of searching out principles of ancient Hindu law and justice Dharmashastra texts emerge as authentic source of information.

On the basis of above study, a developed and established form of governance was found in Dharmashastra treaties and they make an important place in history of governance in Indian perspective.

Mahabharat [67]

In ancient India, during Mahabharat period, Rajadharama, Dandaniti, Arthashastra, Rajyashastra and Nitishastra are some of the most important terms which describe the study of politics. Dandaniti is most frequently used among them. Mahabharat is presumably the first Indian treatise on the science of governance. There is one huge Rajdharama section discussing various aspects of governance besides Sabhaparvam and Vanaparvam. The Rajadharma section constitutes part of Shantiparvam. After the great Mahabharat war, the winning group of Pandavas headed by the eldest of them, Yudhishtira, approached their grandfather Bhishma for guidance in running the administration of the state, particularly good governance. The lengthy discussions were on the functions, duties, role and characteristics of a good, popular and dutiful king.

For good governance, one may refer to the constitution of the Sabha and the qualifications of its members under Mahabharat. Manu prescribed seven or eight ministers, while according to Bhishma in Mahabharata the range was between three and eight. Qualifying criteria have been enumerated: restrained, pride-free, truthful, respectful to superiors, capable, soft-spoken, steady, well-to-do, heroic, pious, grateful, greed-free, contented, knowledgeable, learned, polite, upright, and so on. Very interestingly, the following are forbidden from being present or participating at these meetings: a crooked person, not learned, impure [read dis-reputed], idiots, lunatics, a convicted person, and so on. Confidentiality is stressed, in edicts that lay down leakage of counsel prejudicial to the interest of the kingdom. In addition to what has been cited already, the Mahabharata offers several other inputs into the ideal conduct and characteristics of a king (all of which could be suitably adapted to the modern corporate chief executive). Standing out far and ahead of the detailed listings of these attributes is the concern the king should have for his subjects and the respect and heed that he should extend to his counsellors, who should of course themselves be beyond blemish. The analogy of the king and his subjects to a mother and her child is at once remarkable in its simplicity as well as its telling impact. "As the mother, disregarding those objects that are most cherished by her, seeks the good of her child alone, even so, without doubt, should kings conduct themselves [towards their subjects]." Equally striking is the enumerated criteria for selection of advisors:

“ men that are brave, devoted, incapable of being deceived by foes, well-born, healthy, well-behaved, and connected with families that are well-behaved, respectable, ..” and so on.

The King’s councillors were in a body called the Parishad. In the Upanishads, it means a gathering of specialists discussing problems of philosophy. In Dharma Sastras, the Parishad connotes an advisory body of the king in judicial and, probably also, in administrative affairs. It usually consisted of at least ten members, all well instructed, skilled in reasoning, and free from covetousness. An important point to note in this context is the elevation of society above the individual, and allegiance to Dharma rather than to any particular party or political principle.

The king had his rights and duties, failure to perform led to expulsion or banishment in this world, and to worse perhaps in the next. One could see some linkages to the theoretical suzerainty of the modern corporate board over the executive and its empirical demonstration from time to time in the matter of replacing the chief executive for non performance, as has happened in several instances in the recent past, especially in better developed economies of the world.

In Thiru Kural, we find some telling observations on the king and the importance of his advisors. “A man’s greatest strength is meriting friendship with those greater than himself,” and, “who can destroy the man who enjoys the friendship of aides who will not hesitate to admonish him?”, and again, “With none to reprove and thus protect him, a king will be destroyed, though no one seeks his destruction.” Encouraging contrarian but constructive critiquing by independent directors on corporate boards could, in the modern context, be the saving grace of many a chief executive, especially if he or she is from the dominant shareholding group or family. Even on the selection of appropriate advisors, Thiru Valluvar offers wholesome advise: “Knowing that they function as a monarch’s eyes, a king looks at ministers meticulously before engaging them.” But he does not spare the advisor or the minister either. Having been chosen, what should such functionaries do in the discharge of their duties? “Call him a minister who comprehends things, effectively executes them and competently directs others.” And, “The loyal minister’s duty is to communicate his counsel, even if the leader is a dullard who spurns advice.” The titles of course are different, but one can read the meaning of the counsel that is offered both to the executive and to the non-executive players in modern corporate governance.

Kautilya’s Arthashastra [46, 69]:

Kautilya is even more explicit on governance. According to him “A king can reign only with the help of others; one wheel alone does not move a chariot. Therefore, a king should appoint advisors (as councillors and ministers) and listen to their advice”. Kautilya is paranoid when it comes to verifying why certain advisors hold the views they do and also values individual consultations to collective discussions. “The opinions of advisers shall be sought individually as well as together as a group. The reason why each one holds a particular opinion shall also be ascertained”. Kautilya is quite vehement on the imperatives of the king and his counsellors acting in concert. “If the king and his counsellors do not agree on the course of action, it spells future trouble, irrespective of whether the venture is crowned with success or ends in failure”. There could be no stronger counsel relevant to modern day corporate governance structures for executive managements to heed the advice given by the non-executive independent colleagues on the board of directors.

Kautilya demonstrated an extremely vital imperative of good administration i.e. governance, polity, politics and progress have to be linked to the welfare of the people. Interestingly, closer to recent times, Abraham Lincoln said, “Democracy is for the people, by the people and of the people”. The Arthashastra’s resonant theme holds even truer today and it is the upholding of this principle that stands at the core of attaining development.

Kautilya has also provided an exhaustive and illustrative description of the duties, responsibilities and role of the king, prince(s), ministers, and other state officials. As for the state’s political administration, Kautilya provided a full-fledged commentary as to how this should be effectively undertaken. He gave instructions about the defence of the state’s boundaries, protection of the forts, and the manner in which the invasion by the enemy must be handled.

The Arthashastra classifies legal matters into civil and criminal and it specifies elaborate guidelines for administering justice in terms of evidence, procedures and witnesses. Furthermore, Kautilya strongly believed in Dandniti, though he maintained that penalties must be fair and just, and proportionate to the offence committed.

Further, attainment of good governance entails that the objectives of the state are fulfilled and realized, which is possible only through properly organized and guided administration. This principle is relevant even today. A government is good, if it is administered well. Kautilya suggests that good governance should avoid extreme decisions and extreme actions. Soft actions (Sam, Dam) and harsh actions (Dand, Bhed) should be taken accordingly. Kautilya opines in a most modern way - ‘Sovereignty is practicable only with the cooperation of others

and all administrative measures are to be taken after proper deliberations.’ The King and ministers were supposed to observe strict discipline. Kautilya recommended a strict code of conduct for himself and his administrators. Kautilya has seriously considered the problem of corruption, which is listed, in the Arthashastra, about forty ways of embezzling government funds. However, Kautilya was very practical about the problem of corruption. Kautilya felt that it is as difficult to discover the honesty or otherwise of an officer as it is to find out whether or not it was the fish that drank the water.

Kautilya discusses the problems of governance extensively and provides his prescriptions to address these problems. He addresses the issues pertaining to the king, his ministers and the civil servants. The King should set high standards, and consult with appropriate number of his advisors before taking action. After the ruler has secured the allegiance of his own people and leaders, and reached an understanding with those in enemy territories, he should devote his attention to planning new undertakings.

Arthashastra suggests a highly centralized government for efficient and effective administration with no intermediaries between the farmers and the central administration. Kautilya suggests that state servants should be recruited from far and wide in the kingdom. The work of the Directors and officials should be subject to periodic review. It emphasizes the importance of harmonious teams but also warns against excessive fraternizing because it can subvert the administration and cause financial losses to the state. All three faults in revenue collection (a) not collecting funds that are due, (b) harsh exploitation, and (c) not managing the expense should be avoided. The ruler should receive accurate and complete progress reports on income and expenses in order to make good decisions and policy.

The records-cum-audit office maintains comprehensive records from each department as well as ongoing projects, informs the work officers of various departments and undertakings about the specified dates when they must submit the accounts and balances for audit, and ensures the integrity of the records and information provided by the work officers of the operating departments and their accounts officers. It must check each entry of receipt for the time, place, amount, source, name of recorder, and recipient, and similarly the expense and balance entries must be checked. All such appointments are made by a royal order.

Arthashastra is a treatise which sets out a framework based on clear definition of accounting concepts, and uniform standards but recognizes that the framework is not sufficient to prevent wrongdoing. The proper implementation of rules by the responsible officers who are above favouritism or vindictiveness creates faith in the system. Officers should be carefully selected

for their knowledge, expertise and character, given the importance of the treasury. Even when people are carefully selected, their actions should be constantly reviewed, departments should have many heads, and they should not be given permanent tenure. It defines penalties and fines for preventing various kinds of wrongdoing that short-change the treasury. Finally, Arthaśāstra suggests an intelligence network to watch over the activities of the departments and ascertain whether officials are living beyond their means.

Besides above, Kautilya made explicit provision for whistleblowers (informers) and their protection and rewards to secretly bring the actions to defraud the treasury to the attention of the king. Whistleblowers were not only guaranteed protection against reprisals by the officers, but were to be rewarded with a part of the amount involved if the matter were proved, and punished for false accusations or for failure to appear to prove the charges.

Although in many places Kautilya refers to fixed prices, compensation and fines fixed in terms of money or as multiples of the relevant amounts, he emphatically disagrees with his predecessors by asserting the ultimate dominance of judgment and discretion as a better guide than fixed rules. The debate between fixed rules and discretion has a long history in jurisprudence, economics management and accounting. Fixed rules have the advantage of clarity, fairness, and openness. On the other hand, no set of fixed rules can anticipate all circumstances, and their application can lead to patently unfair outcomes in specific circumstances. In his ambivalence between specific rules for determining fines, and leaving it to the discretion and judgment so the fine will be appropriate to the guilt of the offender, Kautilya reflects the same problem.

In ancient Indian government, one finds the different elements of modern government also. This means that the foundation of the modern day government was laid during the ancient times itself. The ancient Indian government had three major components in the hierarchy structure. They were: *Legislative, Executive and the Judiciary*. The chief head of the three departments was the King. Effective judiciary was made sure that crime was under control and the offenders got the apt punishments for their crimes.

Thus, it may be observed from above discussions that the ancient Indian government had an effective way of keeping tabs on what people thought of the administration. This was kept in check by a very secretive system of spies. The king used to be updated about what is happening in his kingdom regularly by these spies who used to roam around in the kingdom in disguise. There was effective military and the soldiers were well trained in the art of

warfare. There were regular updates of population, birth rate, death rate, etc. Despite a huge empire, administration was controlled and highly effective in ancient India.

Current times accentuate the present applicability of this because the need for a sound and comprehensive state administration has been accentuated by the propensity of the powerful to flout the law and do so repeatedly.

2.3.3 Details of Governance during the Medieval Period - Delhi Sultanate & Mughal India

The medieval period saw the advent of Islam in India and rule of absolute monarchy replaced all earlier forms of governance or government prevalent in ancient India. The Muslim rulers tried to enforce their laws and ideas on the general population and some of the features of their government are prevalent even today like taxation and land reforms.

The administration of Delhi Sultanate and Mughal Dynasty left memorable footprints regarding Governance in India. It is essential to keep in mind to understand the nature of Muslim religion for clear understanding of Governance principles because Islam aimed at the realisation of the practice in the society where only laws of God prevailed. Especially in Delhi Sultanate Alauddin Khilji made a significant contribution regarding Governance. He made far-reaching changes in the Administrative and Revenue reforms. Market control regulations were introduced and a lot of conquests took place during his reign. Alauddin's reign is considered the best under the Khilji rule.

The Mughal empire provided a system of government that shared many ideas with the Sultanate as well as bringing in some new ideas of its own. It also incorporated many Indian ideas as well. The empire was essentially still military in nature, with every officer of the Mughal state a member of the army. The emperor was an autocrat and had unlimited freedom in making laws. Although he had a council of ministers, he was not bound to consult them, and his word was law. The only restriction was that he had to follow the guidelines set forth in the scriptures and Islamic traditions. However, a powerful emperor could often violate these as well. The great Mughal kings can best be described as benevolent despots, who ruled fairly and justly. Most of them did involve their ministers in decision making. They also attempted to improve the lives of their subjects, although there was no socialistic work in their times.

The administrative system of the Mughal Empire was largely the work of Akbar, for the early two Mughal kings (Babur and Humayun) did not really get the chance to implement much of a

system. Akbar's task was simplified for he inherited some measure of Sher Shah's system of organization. During Akbar's time the system worked very well, but it began to deteriorate during the time of his successors. As mentioned earlier, all officers were members of the army. Each officer was assigned a specific responsibility, and was paid a monthly salary. He was also required to maintain a certain strength of troops, with senior officers commanding larger units and drawing greater salaries. The system was very flexible and an officer could be assigned to any office. During Akbar's time, the system worked very well because of Akbar's remarkable ability to pick the right man for the right job, though such efficiency slowly deteriorated during the reign of his successors. The officers were either paid their salaries in cash or were granted land for short periods of time, on which they could obtain revenue.

The empire was administered by a number of departments with officers assigned to each of them. The main departments of the state were:

- The Exchequer
- Accounts and Salaries
- Judiciary
- Charities
- Public morals

The highest officer was the *Wazir* (chief minister), followed by the *Bakshi* who was responsible for the salaries of all the employees of the state. He was also involved in recruitment for the army as well as recruiting officers for the administration. There were various other departments and officers like the Auditor General, the head of the Imperial workshop, the superintendent of forests, the news reporters etc.

The revenue system is an important part of any government and the Mughals had a fairly well organized system of revenue collection. Land revenue continued to remain an important source of income for the state. Other sources were trade, industry, transport etc. Around the time Akbar ascended the throne the land revenue system was fairly disorganized with a mix of nobles, landlords etc. involved in land ownership and revenue collection. Akbar realized the importance of an efficient land revenue policy for an expanding empire. Initially he tried out a disastrous experiment, which eventually had to be cancelled. He attempted a new system, in which he first abolished all current land holdings. The empire was then divided into a series of land holdings, each yielding a fixed amount of revenue every year. These areas were then allotted to an officer called a *Krori*, whose job was the collection of revenue and encourage cultivation (which in turn would boost revenue). However the *Krori's* turned out to be corrupt tyrants at whose hands the cultivators went through tremendous suffering. The system was quickly abolished and the

earlier system restored. In 1852 AD an important new development took place in the re-organizational effort of land revenue. Todar Mall was appointed to the post *Dian-I-Ashraf* . A new system was established which had three divisions.

- A survey to measure land
- The classification of the various types of land (degree of fertility etc)
- An annual survey to determine the rate of taxation.

The system was essentially fair, as the land would be only assessed for the portion where cultivation was done. The tax was one third of the produce, and the landlords could pay the tax in either cash or kind. The monetary value of the crops varied depending on the type of crop and the prevailing market conditions.

To assist in the purposes of administration and revenue collection, the Mughal Empire was divided into a hierarchical system of areas. The empire was first divided into a number of *subahs* . The *subahs* were then divided into *paraganas* . A *paraganas* was a union of several villages. At each stage there were several officers who supervised operations like revenue assessment and collection etc. Their orders were to collect revenue in a just and efficient manner and not put undue pressure on villagers, especially if they had suffered a natural disaster. Apparently there was tremendous accountability, because we have records of even high ranking officials like provincial governors being dismissed after complaints were made against them by the citizens. The entire system worked fairly well, the landlords now had a sense of security with a developed system and were given a fair amount of flexibility in paying their dues. Although the tax rate was on the higher side (one third of the total produce) it was pretty reasonable considering the emperors abolished various other taxes.

During the time of the Mughal Empire there was no formal written law, but there was a keen interest amongst the Mughal emperors to deliver speedy justice to its citizens. The justice system placed even senior officers within the law, and perhaps the only person really above the law was the emperor himself. The Mughal emperors were very keen on justice, but for most of the Mughal period, appealing to the emperor was a complex procedure. Two notable exceptions were Akbar and Jehangir, who allowed subjects to directly petition them. In addition to the emperor there were other officers in charge of justice. The chief justice was known as the *Quazi-ul-Quazat* . He was in charge of maintaining the judicial system throughout the empire. For this purpose he was responsible for the appointment and management of *Quazi's* all over the empire. Under them there were no lower courts. Most villagers however resolved their cases in the village courts itself. The punishments were fairly severe, ranging from imprisonment to

amputation, mutilation and whipping. The approval of the emperor was however mandatory for capital punishment. In the Mughal judicial system, the emperor was the final court of appeal.

Whilst the Mughal empire was able to once again provide an organized government to India, it failed to recapture the effectiveness and efficiency of those governments from the time of the Mauryas and Guptas. Hence they were able to unite India only under an empire, not under a government. This proved to be a serious fatal flaw, because after the decline of the greater Mughals, the already autonomous regions of the empire declared themselves independent. This presented a fractured and divided country to the Europeans, which made their task of conquering India a much simpler one.

The principles of Mughal government, their policies, and rules of taxation, departmental arrangements and the very titles of their officials were imported, ready-made from outside of India. The existing Indian practices and vast mass of Indian customary law were respected, as they did not run counter to the basic principles of all Islamic governments.

2.3.4 Governance structure during British India [30]

The British Government took over the administration of India from the East India Company by the Government of India Act, 1858. Thereafter, the British Parliament enacted several laws for governance of India. Some of the important legislative instruments in the pre-independence period were the Indian Councils Act, 1909; Government of India Act, 1919; and Government of India Act, 1935. With India attaining Independence, the constitution of India laid the foundation of the structure of Government of India.

With the Government of India Act, 1858, the erstwhile territories of the East India Company vested in the British Crown who would appoint the Governor General of India as well as the Governors of the Presidencies. The powers of the Crown were to be exercised by the secretary of state for India, assisted by the Council of India.

The Indian civil service was created consequent to this enactment. There was no popular participation in the governance system.

The Indian Councils Act of 1909, also known as the Morley-Minto Reforms, introduced the elections of Indians to the legislative councils. The Government of India Act, 1919, also known as the Montague Chelmsford Reforms, introduced a dual form of government ("Diarchy") for some provinces - the reserved list and the transferred list.

The Government of India Act, 1935 brought several changes in the system of governance in the country. It provided for the establishment of an All-Indian Federation and a new system of government wherein the provinces were given more autonomy.

The central legislature was to comprise two Houses - the Upper House or the council of states and the Lower House or the central legislative Assembly. The 'Diarchy' which was earlier established in the Provinces was abolished but was introduced in the centre.

The executive authority of the centre was vested in the Governor General (on behalf of the crown) who had absolute power over Defence, External Affairs (Reserved subjects). On other matters the Governor General was to act on the advice of a "Council of Ministers".

The Act stipulated that no Finance Bill could be placed in the central legislature without the consent of the Governor General. The Act further provided for three lists -

- (a) To the exercise of such rights, authority and jurisdiction as are exercisable by the Government of India by virtue of any treaty or agreement: Provided that the executive power referred to in sub clause.
- (b) Shall not, save as expressly provided in this Constitution or in any law made by Parliament, extend in any State to matters with respect to which the Legislature of the State has also power to make laws.
- (c) Until otherwise provided by Parliament, a State and any officer or authority of a State may, notwithstanding anything in this article, continue to exercise in matters with respect to which Parliament has power to make laws for that State such executive power or functions as the State or officer or authority thereof could exercise immediately before the commencement of this Constitution.

2.3.5 Post Independence India

The country became an independent dominion within the British Commonwealth on 15 August 1947. The history of the Republic of India began on 26 January 1950 where the central and states structure of governance was defined with three important pillars of democracy i.e. Legislature, Executive and Judiciary to function on the principles of checks and balances for effective governance and welfare of the citizens of the country. Although, the basic framework of the Administration was the legacy of British system of Governance in India but a comprehensive exercise was done by the constituent assembly under the Chairmanship of Dr. B. R. Ambedkar after examining a number of constitutions of the

different countries of the world. Our constitution provides full flexibility to meet the requirement of the country in the changing circumstances. It is the longest written constitution of any independent nation in the world, containing 395 articles and 12 schedules, as well as numerous amendments, for a total of 117,369 words in the English language version.

The Constitution lays down the basic structure of government under which the people are to be governed. It establishes the main organs of government - the executive, the legislature and the judiciary. The Constitution not only defines the powers of each organ, but also demarcates their responsibilities. It regulates the relationship between the different organs and between the government and the people.

The Constitution is superior to all other laws of the country. Every law enacted by the government has to be in conformity with the Constitution. The Constitution lays down the national goals of India - Democracy, Socialism, Secularism and National Integration. It also spells out the rights and duties of citizens.

The Constitution applies to the State of Jammu and Kashmir with certain exceptions and modifications as provided in article 370 and the Constitution (Application to Jammu and Kashmir) Order, 1954.

Features of Indian Constitution and the Governance

To understand the mechanism and structure of Governance [10], it is essential to know the basic features of Indian Constitution. The Constitution of India draws extensively from Western legal traditions in its enunciation of the principles of liberal democracy. It is distinguished from many Western constitutions, however, in its elaboration of principles reflecting aspirations to end the inequities of traditional social relations and enhance the social welfare of the population. According to constitutional scholar Granville Austin, probably no other nation's constitution "has provided so much impetus toward changing and rebuilding society for the common good." Since its enactment, the constitution has fostered a steady concentration of power in the hands of the central government - especially the Office of the Prime Minister. This centralization has occurred in the face of the increasing assertiveness of an array of ethnic and caste groups across Indian society. Increasingly, the government has responded to the resulting tensions by resorting to the formidable array of authoritarian powers provided by the Constitution. However, a new assertiveness shown by the Supreme Court and the Election Commission suggests that the remaining checks and balances among the country's political institutions are resilient and capable of supporting Indian democracy. Furthermore regional parties are gaining popularity at the expense of national parties which

has led to coalition governments at the centre. As a consequence, power is becoming more decentralised.

The Constitution in its final form owes much to a number of different principles from various other Constitutions. The general structure of the Constitution's democratic framework was largely the work of B. N. Rau, a constitutional scholar of international standing. Supporters of independent India's founding father, Mohandas K. Gandhi, backed measures that would form a decentralized polity with strong local government — known as panchayat — in a system known as Panchayati Raj, i.e. rule by Panchayats. However, the view of more modernist leaders such as Jawaharlal Nehru, ultimately prevailed leading to the establishment of a parliamentary system of government and a federal system with a strong central government.

Schedules

Schedules can be added to the constitution by amendment. The twelve schedules in force cover the designations of the

1. States and Union Territories;
2. Emoluments for High-Level Officials;
3. Forms of Oaths;
4. Allocation of the number of seats in the Rajya Sabha (Council of States - the upper house of Parliament) per State or Union Territory;
5. Provisions for the administration and control of Scheduled Areas and Scheduled Tribes (areas and tribes needing special protection due to disadvantageous conditions);
6. Provisions for the administration of tribal areas in Assam;
7. The Union (central government), State, and Concurrent (dual) lists of responsibilities;
8. The Official Languages;
9. Article 31B-Validity excluded from Court's Review (land and tenure reforms; the association of Sikkim with India);
10. Anti-Defection provisions for Members of Parliament and Members of the State Legislatures;
11. Panchayat Raj (Rural Development);
12. Municipality (Urban Planning).

Amendments

Methods of Amendment

- By simple majority of the Parliament: Amendments in this category can be made by a simple majority of members present and voting, before sending them for the President's assent.
- By special majority of the Parliament: Amendments can be made in this category by a two - third majority of the total number of members present and voting, which should not be less than half of the total membership of the house.
- By special majority of the Parliament and ratification of at least half of the state legislatures by special majority. After this, it is sent to the President for his assent.

On paper, an amendment to the Constitution is an extremely difficult affair, and normally needs at least two-thirds of the Lok Sabha and Rajya Sabha to pass it. However, the Constitution of India is one of the most frequently amended constitutions in the world. Many matters that would be dealt with by ordinary statutes in most democracies must be dealt with by constitutional amendment in India due to the document's extraordinary detail. The first amendment came only a year after the adoption of the Constitution and instituted numerous minor changes. Many more amendments followed, at a rate of almost two amendments per year since 1950. Most of the Constitution can be amended after a quorum of more than half of the members of each house in Parliament passes an amendment with a two-thirds majority vote. Articles pertaining to the distribution of legislative authority between Union and State governments must also be approved by fifty percent of State legislatures.

In 1974, the Supreme Court of India in the landmark case of *Kesavananda Bharati vs. The State of Kerala* enunciated the Basic Structure Doctrine, which expanded the scope of judicial review to include the power to review Constitutional Amendments passed by the Legislature. Using this doctrine, the Supreme Court has struck down the 39th Amendment and parts of the 42nd Amendment as being violative of the Basic Structure of the Constitution. Some noted authors of Constitutional law, such as HM Seervai have argued that this is an usurpation of amending power by the judiciary, which was never intended by the framers of the Constitution. However, it can be argued that this doctrine is necessary to protect human rights from being abrogated simply by constitutional amendment. There have been a total of 97 amendments to the constitution of India, till January 2012.

2.4 Summary

Ancient civilisations across the globe have seen many forms and principles of Governance. It relates to decisions that define expectations, grant power, or verify performance. There was always a need for smooth administration and division of responsibilities. Since the population started to increase, people grew concerned about welfare and able ruling. This led to the rise of an organizational structure that dealt with the nuances of firm ruling and governance.

After independence India began to plan carefully its needs and resources. Planned economic development was the call of the hour. The focus was on developing large scale and heavy industries. The state controlled the economic policies of development. A blend of liberalization, privatisation and globalisation was pursued to achieve desired results. The economy was essentially mixed in nature with a blend of capitalism and socialism that has led India to the present state [6].

A need was felt for effective and efficient Governance after so many years of independence. There is a change in thinking of definition and composition of concept of Governance. The involvement and participation of the people at all stages of planning, implementation and monitoring is a pre-requisite for good Governance. Very often plans are misplaced because they are not reflective of the actual requirements of the people and are not culturally and socially sensitive to the ethos of the people for whom they are meant. People must feel a sense of ownership of such plans/programmes and must participate and even contribute towards them.

With the advent of new technologies around the globe, Information and Communications Technologies (ICT) has taken a lead role and has become one of the most sought and used technologies in the life of citizens. During the last two decades of globalisation and liberalisation along with the revolution in ICT and knowledge-based environment, there is a change in thinking of definition and composition of concept of Governance.

e-Governance comprises the use of ICTs to support public services, government administration, democratic processes, and relationships among citizens, civil society, the private sector, and the State. e-Governance has been an emerging idea and is based on the rejection of bureaucratic governance that was not responsive to the imperatives of knowledge society. It is not just about a website and a digitisation of service delivery mechanism. It certainly stands on a greater definition of engagement and depth of relationship that surrounds

both the citizens and the government. Citizens are now looking for more trust, accountability, transparency and quick delivery of services in a time bound manner.

In the next chapter the inception and evolution of e-Governance has been discussed.

Evolution of e-Governance

3.1 Introduction

In his *Grundlegung Zur Metaphysik de Sitton*, Immanuel Kant says, “*So act as to treat humanity, whether in their own person or in that of any other, in every case as an end withal, never as means only*”. Kant’s observation is relevant even in today’s world. Various stakeholders like citizens and businesses are ends in themselves, rather than as means to other ends. In colonial times, government was viewed as a “controller” and “ruler”. Government’s role is now that of a coordinator and provider; it is responsible for providing specific services to citizens and businesses, just like an organization is responsible for managing a value chain that leads to output.

The primary purpose of governance is the welfare of citizens. While one aspect of governance relates to safeguarding the legal rights of all citizens, an equally important aspect is concerned with ensuring equitable access to public services and the benefits of economic growth to all. The components of governance include an input mechanism, a data repository, a processing methodology, and an output mechanism. In traditional governance systems, data repository is in the form of a pile of physical files in geographically distributed offices of the government. Input usually comes in the form of paper applications and forms, along with optional payments, from stakeholders. These are processed manually by the hierarchy of government officers and employees. The output is generated in the form of government orders, certificates, payments, etc. These manual procedures usually encourage discretion, delay and corruption on the part of government officers and employees. The stakeholders are forced to physically visit various offices and departments for different service requirements. As a whole, this results in an inefficient delivery system and causes harassment to the stakeholders.

Efficient governance requires efficient institutions. The efficiency and effectiveness of institutions, in turn, depends on their adopted delivery mechanism and the supportive framework of rules and procedures, each of which has to work in harmony with the other to discharge the functions for which the institutions have been created. Only then would one expect the institutions to fulfill their stated objectives and carry out their assigned responsibilities in managing the affairs of the society. More importantly, with the changing

context – domestic as well as global – a change in the profile and requirements of society and development, there has to be a capacity for evolution, a continuous adaptation in each of these elements

Experience shows that while good governance can help secure human well being and sustained development, it is equally important to recognise that poor governance could well erode the individual capabilities, as well as institutional and community capacities to meet the needs of sustenance.

3.2 Use of ICT in Governance

Information and Communication Technology (ICT) [14] is the tools and techniques used to capture, store, manipulate, communicate and use information. Fully exploiting the capability of ICT is of critical importance to the delivery of modern government and businesses in a knowledge-driven economy. (ICT) plays a critical role in speeding up the flow of information and knowledge between government and citizens and transforming the way in which governments and citizens interact. According to the United Nations Development Programme (UNDP) the challenge for all countries is to create and develop a system of governance that promotes, supports and sustains human development. Governments in many parts of the world including India have made huge ICT investments aimed at improving governance processes.

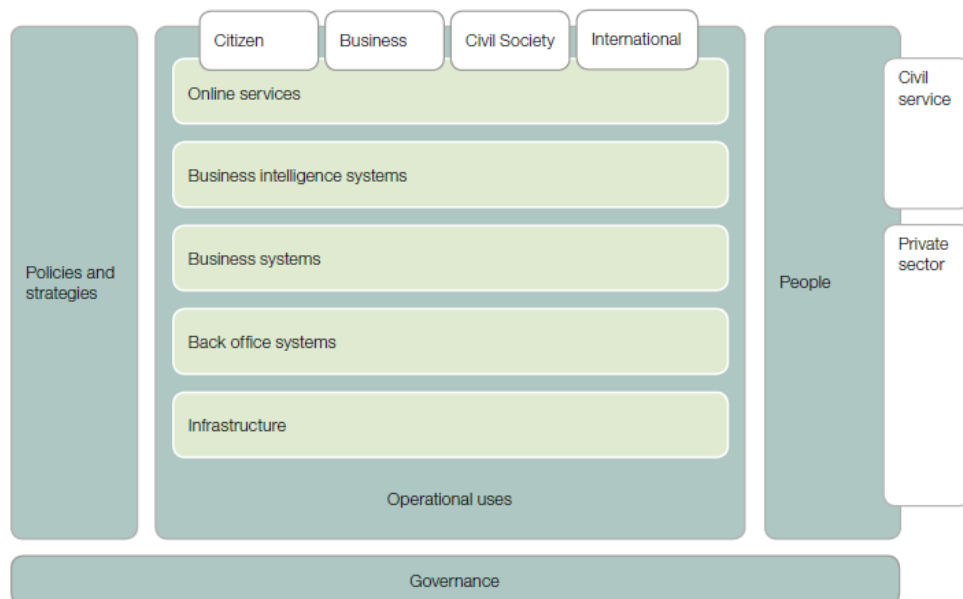


Figure 3.1: Key Components of Government ICT

Figure 3.1 shows a simple representation of the four key components of government ICT: **policies and strategies, its operational uses, people and governance**. It is the interaction of all of these that influences value for money.

3.2.1 Policies and strategies

Across government there is a broad range of policies that underpin how ICT is used in public services, how it is developed and ultimately brought into operation. This includes business policies on transparency of information and how it is managed and secured, commercial policies on strategic supplier relationships and more technical policies relating to common standards for ICT [3].

3.2.2 Operational Uses

ICT is used in many ways across government but five broad applications are generally recognized. These are:

Online services: A growing number of public services are now available online, reflecting trends in the private sector and the need to reduce the costs of delivering services. Citizens and businesses are able to use the Internet to file tax returns, make benefit claims, apply for immigration visas, renew vehicle road tax, apply for passports or book medical appointments. Websites guide citizens and businesses to the information they need and the External Affairs Office uses the Internet to disseminate overseas travel advice.

Business intelligence systems: These systems typically automate the collation, analysis and presentation of financial information, management information and metrics about business performance and relevant progress indicators across an organization. When combined with effective systems for budgeting, planning, forecasting and optimization, business intelligence systems provide the means to navigate through and share management information across an organization and are key to informed decision-making in knowledge-intensive organizations.

Business systems: These systems sit at the heart of public service delivery. They can range from simple database applications through to large transactional systems supporting the operation of tax collection and benefits payments. Many areas of government have been made more efficient through the deployment of business systems, but these have also presented the biggest challenges to value for money. Usually business systems are developed from scratch by large IT suppliers to deliver very specific and customized solutions for government.

Back office systems: Every public sector body relies on a range of finance, human resources, procurement and facilities management systems to manage its operations effectively. These systems deliver core functions that all organizations need for strong financial control.

Infrastructure: ICT provides all of the basic tools for the modern working environment. Desktops, printers, laptops, telephones, servers, software applications and email are all necessary for efficient government operations. They are ICT commodities that are available from the market. Infrastructure can directly affect other costs such as office accommodation. It influences how productive and mobile the front line and civil service workforce is, and the extent to which flexible and collaborative working is possible.

3.2.3 People

The people involved in government ICT include change specialists, business strategists and analysts, as well as the more traditional systems architects, software engineers, service managers and database administrators. ICT professionals are responsible for the continuous design of operating models and business processes to take advantage of rapidly evolving technology. Successful organizations will typically rely on them as a central part of strategic decision-making and design of new services, not just for applications development and the running of operating systems.

3.2.4 Governance

ICT governance is the people, systems and processes that direct, approve, control and assure an organization's ICT. It operates both across government and within government bodies.

3.3 Concept of e-Governance

e-Governance is the application of ICT for delivering Government Services, exchange of information, communication transactions, integration various stand-alone systems and services between Government and Citizens (G2C), Government and Business (G2B) as well as back office processes and interactions within the entire Government frame work. Common interactions in e-Governance have already been introduced in section 1.3. Through e-Governance, government services will be made available to the citizens in a convenient, efficient and transparent manner. The Government being the service provider, it is important to motivate the employees for delivering the services through ICT. To achieve this, the Government employees are being trained on technology and started realizing the advantage of

ICT. The aim is to make them thorough with e-Governance applications and responsive to the technology driven administration.

Defined broadly, e-Governance is the use of ICT to promote more efficient and effective government, facilitate more accessible government services, allow greater public access to information, and make government more accountable to citizens. e-Governance has emerged beyond electronic service delivery and is part of the ongoing reform and transformation of government enabling participatory governance and partnerships to improve efficiency and effectiveness [5]. e-Governance is about transforming government to be more citizen-centered. Technology is a tool in this effort. e-Governance successes require changing how government works, how it deals with information, how officials view their jobs and interact with the public.

e-Governance comprises the use of ICTs to support public services, government administration, democratic processes, and relationships [23, 37] among citizens, civil society, the private sector, and the state. Developed over more than two decades of technology innovation and policy response, the evolution of e-Governance is examined in terms of five interrelated objectives: a policy framework, enhanced public services, high-quality and cost-effective government operations, citizen engagement in democratic processes, and administrative and institutional reform. This summary assessment of e-Governance in U.S. states and local governments shows that the greatest investment and progress have been made in enhanced public services and improved government operations. Policy development has moved forward on several fronts, but new policy issues continually add to an increasingly complex set of concerns. The least progress appears to have occurred in enhancing democracy and exploring the implications of e-Governance for administrative and institutional reform. ICT-enabled governance will continue to evolve for the foreseeable future providing a dynamic environment for ongoing learning and action.

Different experts and institutions have defined e-Governance but before presenting an overall definition of e-Governance, it is essential to understand the relation between governance, e-democracy and e-Government.

E-democracy refers to the processes and structures that encompass all forms of electronic interaction between the Government (elected) and the citizen (electorate) whereas e-Government is a form of e-business in governance and refers to the processes and structures needed to deliver electronic services to the public (citizens and businesses), collaborate with business partners and to conduct electronic transactions within an organizational entity.

According to a research report no. 3, April 2001 on “e-Governance and Developing Countries- Introduction and examples” by Michael Backus e-Governance is defined as the application of electronic means in

(i) The interaction between government and citizens and government and businesses, as well as and (ii) Internal government operations to simplify and improve democratic, government and business aspects of Governance.

As per above definition of e-Governance, the term interaction stands for the delivery of government products and services, exchange of information, communication, transactions and system integration. Government consists of levels and branches. Government levels include central, national, regional, provincial, departmental and local government institutions. Examples of government branches are Administration, Civil Service, Parliament and Judiciary functions. Government operations are all back-office processes and inter-governmental interactions within the total government body. Examples of electronic means are Internet and other ICT applications.

Hence, e-Governance is fast emerging as an important tool for achieving good governance especially with regard to improving efficiency, transparency and making interface with government user friendly. So far the emphasis has been on providing connectivity, networking, technology upgradation, selective delivery systems for information and services and a package of software solutions.

3.3.1 e-Governance objectives

The strategic objective of e-Governance is to support and simplify governance for stake holders i.e. government, citizens and businesses. The use of ICTs can connect all three parties and support processes and activities. In other words, in e-Governance electronic means is used to support and stimulate good governance. Therefore, the objectives of e-Governance are similar to the objectives of good governance. Good governance can be seen as an exercise of economic, political, and administrative authority to better manage affairs of a country at all levels, national and local.

The two main objectives of e-democracy are:

(i) To provide citizens access to information and knowledge about the political process, about services and about choices available and

(ii) To make possible the transition from passive information access to active citizen participation by:

- Informing the citizen
- Representing the citizen
- Encouraging the citizen to vote
- Consulting the citizen
- Involving the citizen

Regarding e-Governance, the distinction is made between the objectives for internally focused processes (operations) and objectives for externally focused services.

External strategic objectives: The external objective of e-Governance is to satisfactorily fulfill peoples' needs and expectations on the front-office side, by simplifying their interaction with various online services. The use of ICTs in government operations facilitates speedy, transparent, accountable, efficient and effective interaction with the public, citizens, business and other agencies.

Internal strategic objectives: In the back-office, the objective of e-Governance in government operations is to facilitate a speedy, transparent, accountable, efficient and effective process for performing government administration activities. Significant cost savings (per transaction) in government operations can be the result.

It can be concluded that e-Governance is more than just a Government website on the Internet. Political, social, economic and technological aspects determine e-Governance.

3.3.2 Principles of good governance

Five principles underpin good governance: openness, participation, accountability, effectiveness and coherence.

Openness: The Government should work in a more open manner. Together with the State Governments, they should actively communicate about what the Center does and the decisions it takes. They should use language that is accessible and understandable for the general public. This is of particular importance in order to improve the confidence in public at large.

Participation: The quality, relevance and effectiveness of Government policies depend on ensuring wide participation throughout the policy chain – from conception to implementation. Improved participation is likely to create more confidence in the end result and in the Institutions which deliver policies. Participation crucially depends on central governments following an inclusive approach when developing and implementing government policies.

Accountability [1]: Roles in the legislative and executive processes need to be clearer. Each of the Government Institutions must explain and take responsibility for what it does in the country. But there is also a need for greater clarity and responsibility from States and all those involved in developing and implementing Government policy at whatever level.

Effectiveness: Policies must be effective and timely, delivering what is needed on the basis of clear objectives, an evaluation of future impact and, where available, of past experience. Effectiveness also depends on implementing Government policies in a proportionate manner and on taking decisions at the most appropriate level.

Coherence: Policies and action must be coherent and easily understood. The need for coherence in the Government is increasing: the range of tasks has grown; enlargement will increase diversity; challenges such as climate and demographic change cross the boundaries of the sectoral policies on which the Government has been built; regional and local authorities are increasingly involved in Government policies. Coherence requires political leadership and a strong responsibility on the part of the Government to ensure a consistent approach within a complex system.

Each principle is important by itself. But they cannot be achieved through separate actions. Policies can no longer be effective unless they are prepared, implemented and enforced in a more inclusive way.

3.3.3 Advantages of e-Governance [7]

There are numerous potential advantages related to the implementation of e-Governance such as (Figure 3.2 [30]):

- Lower overall administrative costs to government
- Provide more efficient government operations
- Create a stronger and closer relationship between citizens and government
- Provide easier access to government for all
- Improve the level of service to citizens

- Allow greater access to decision-making
- Empowerment of citizens
- Provide more transparency in government with more responsibility

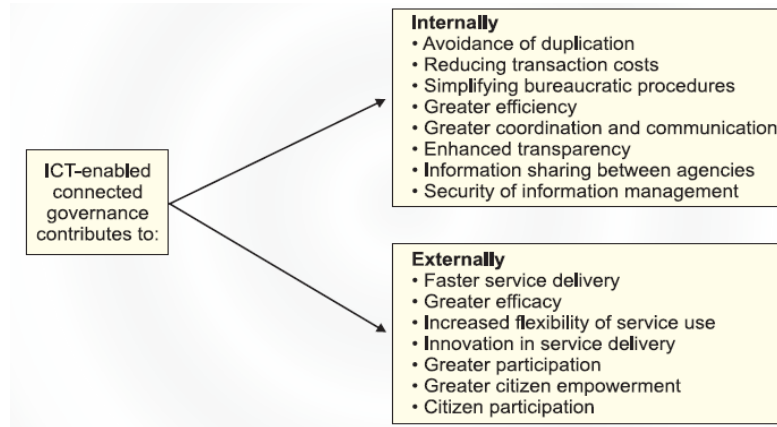


Figure 3.2: Advantages of e-Governance

The main advantages presented by e-Governance to public can be summarized as follows: paper reduction [26], transaction efficiency, and improved governance. As we know, Governance refers to the systems, methods and procedures that define how a government operates. Improved governance and increased accountability is possible through the inclusion of societal participants in the major activities of governments. e-Governance provides the tools for increasing transparency in public administration.

Information in the hands of citizens makes them more connected to government and aware of internal processes that may initially have been perceived as a black box. When a citizen is able to access information, forms and reports, and execute transactions themselves in real-time, they achieve greater ownership of the process. The Internet provides the platform for active participation in government, as well as an avenue for activism and lobbying that can affect the political process. Participation by a large number of interest groups can improve overall governance in a particular region or country.

In a democratic society, increased transparency, as it relates to public policy, is generally perceived as a positive outcome. However, in more restricted societies, control of the Internet and Web-based activities is used as a tool for maintaining government control and affecting governance. Improved governance is thus an advantage of e-Governance that is constrained by the societal and political norms of the region in which it is implemented.

3.3.4 Impact of ICT on Governance

The use of ICT means Governance has impact on the following aspects:

24/7 Service Model

Systems and processes have to be adapted to a completely new service model. Intake processes are made self-service and even in the middle of the night a citizen should get an immediate (automated) response about the status of the application. Citizen's expectations towards government's response times will change because of the new communication medium. E-mail is being used as a new but serious channel besides the traditional channels such as telephone, physical counter, post and fax.

Need for Content

Websites consist of content (information). Governments will have to collect (buy), produce and update content daily. Content managers in each (large) department are responsible for the information on the website.

Human Resources

Effective use of ICTs in an organisation requires training of people. People should feel comfortable with the tools they use otherwise they will return to their old working patterns and habits. Maintaining technological infrastructure requires IT skilled resources. Governments will have to compete with the private (commercial) sector to recruit the necessary IT skilled people.

Security

Just about any computer system is vulnerable to external attacks. As the government moves its core processes (information, communication and transactions) to the Internet, it is becoming far more vulnerable. Internet increases the number of entry points exponentially. Protection is possible with anti-virus software, firewall at gateways, encryption technology, and identification & authentication tools.

Privacy

Governments possess detailed information about citizens and businesses, which is often held in multiple offices on many different computer systems (or still in paper files). The integration of data can result in situations where the privacy of individual citizens is in danger. It is the responsibility of the government to restrict the utilization of private

information, and secure such information from access by unintended parties. Due to public concern regarding privacy several countries have already passed data protection laws.

IT Department

ICTs are key elements supporting the growth of e-Governance initiatives. With the implementation of e-Governance, IT is becoming more and more important in government operations. The need for a professional IT department will inevitably increase, not only during implementation, but also for maintenance of software, hardware and infrastructure for sustainability.

3.4 e-Governance Models

The three main target groups that can be distinguished in e-Governance concepts are government, citizens and businesses/interest groups. The external strategic objectives focus on citizens and businesses and interest groups, the internal objectives focus on government itself.

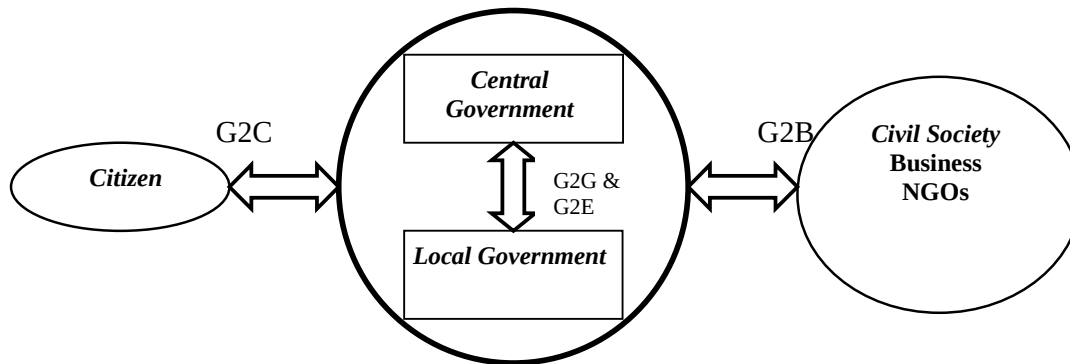


Figure 3.3: Interactions between main groups in e-Governance

The most common group interactions in e-Governance are presented schematically in Figure 3.3. The three abbreviations in the figure, G2C, G2B, and G2E are explained in Table 3.1.

Table 3.1: Main group interactions in e-Governance

	e-democracy	e-government
External		
G2C: Government to Citizen	X	X
G2B: Government to Business		X
Internal		
G2G: Government to Government		X
G2E: Government to Employee		X

Different experts and institutions have developed different e-Governance Models as per requirements of different systems [11]. Some of the important models are described below.

3.4.1 UN Approach

There are 5 stages of e-Governance according to United Nations:

- **Emerging:** In this phase a government web presence is established through a few independent official websites and the information will be limited, basic and static (G2C and G2B). The value to the public is that the information is publicly accessible. Internally (G2G) the government can also disseminate information with static electronic means.
- **Enhanced:** The content and information on these government portals will be updated regularly to give the citizen the up to date information. In this phase the processes are described and thus become more transparent, this improves democracy and service.
- **Interactive:** In this phase interaction between the government and the public (G2C and G2B) is stimulated with various applications. The citizens will be able to download forms, contact officials and make appointments and requests online which previously would have been only possible with long queues near counters. Internally (G2G) the government organizations can use LAN, WAN, intranet and e-mail to exchange information. The citizens can give their feedback and some suggestions on some policy decisions etc. This will bring a sense of participation for the citizen and improves the confidence of the citizen in the government.
- **Transactional:** In this phase, users can actually pay for services or conduct financial transactions online. That is, all the transactions are done online without the citizen going to the office to finalize the decision. In this phase, internal (G2G) processes have to be redesigned to provide good service. Government needs to create new laws and legislation that will enable paperless transactions with legal certification.
- **Seamless:** Under this phase a total seamless integration of e-functions and services across administrative and departmental boundaries. That is the public can get G2C and G2B services at one virtual counter. One single point of contact is the ultimate goal. This needs a drastic change in the culture, processes and responsibilities within

the government (G2G). Government employees in different departments have to work together in a smooth and seamless way. In this phase cost savings, efficiency and customer satisfaction are reaching highest possible levels.

3.4.2 Gartner Approach

Gartner (an international e-business research consultancy firm) has developed an e-Governance Model also known as the e-Governance maturity model. This e-Governance model can serve as a reference for governments to position where a project fits in the overall evolution of an e-Governance strategy.

According to Gartner, e-Governance will mature according to the four-phase e-Governance maturity model (Table 3.2). It has the following four phases:

- Information
- Interaction
- Transaction
- Transformation

These phases have been defined based on experiences with e-commerce and e-Governance in Europe and other Western regions.

Table 3.2: e-Governance Maturity Model (Gartner)

	e-democracy	e-government
Early 90's	Information	
Mid 90's	Interaction	
Present	Transaction	
Future		Transformation

In each of the four phases, the delivery of online services and use of ICTs in government operations serve one or more of the aspects of e-Governance: democracy, government, business. The model does not mean that all institutions have to go through all phases and all at the same time. On the contrary, in the Western world government institutions are in phase 1, 2 or 3. The differences can be huge: the tax department can be in phase 3, while the department of public works is just in an early stage of phase one. It all depends on where the advantages are highest.

Here it should be seen that this model shows four phases for different e-Governance (e-democracy and e-government) solutions. The assumption is made that the government has already defined an overall vision and e-policy.

This is similar to the UN model except that the “Emerging” and “Enhanced” phases which are clubbed to form the Information phase in the Gartner model. The complexity will increase when going from one phase to the other.

Information Phase

In the *first phase*, e-Governance means being present on the web, and providing external public (G2C and G2B) with relevant information. The format of the first government websites is similar to that of a brochure or leaflet. The value to the public is that government information is publicly accessible; processes are described and thus become more transparent, which improves democracy and service.

Internally (G2G) the government can also disseminate information with static electronic means, such as the Internet. This phase it is all about information. From a one-page presence website to a site with all relevant government information available to the public, in order to improve transparency in democracy.

Table 3.3: Examples of Government Information

Examples of information that Government ...		
... wishes to disseminate	... may make available	... is required to supply
press notices consultation papers policies white papers news health and safety advice benefits and entitlements applicable regulations	geographical data demographic data economic data information collected information generated routinely value added services business yellow pages	performance indicators environmental indicators audited accounts personal data internal policy documents correspondence management reports

Interaction Phase

In the *second phase* the interaction between government and the public (G2C and G2B) is stimulated with various applications. People can ask questions via e-mail, use search engines for information and are able to download all sorts of forms and documents. These functionalities save time. In fact the complete intake of (simple) applications can be done online 24/7. Internally (G2G) government organizations use Local Area Networks (LAN), intranets and e-mail to communicate and exchange data.

The bottom line is that more efficiency and effectiveness is achieved because a large part of the intake process is done online. However, one still have to go to the office to finalize the

transaction, by paying a fee, handing over evidence or signing papers. The use of electronic communications tools speed up the internal government processes.

Transaction Phase

With *phase three* the complexity of the technology is increasing, but customer (G2C and G2B) value will also be higher. Complete transactions can be done without going to an office. Examples of online services are filing income tax, filing property tax, extending/renewal of licenses, visa and passports and online voting. Phase three is mainly complex because of security and personalization issues – e.g., digital (electronic) signatures are necessary to enable legal transfer of services. On the business side the government is starting with e-procurement applications.

In this phase, internal (G2G) processes have to be redesigned to provide good service. Government needs to create new laws and legislation that will enable paperless transactions with legal certification. The bottom line is that now the complete process is online, including payments, digital signatures etc. This saves time, paper and money.

Table 3.4: Overview of e-Governance solutions for each phase

Phase	External: G2C	External: G2B	Internal: G2G
Information Phase	Local/Departmental/National information mission statements and organizational structure Addresses, opening hours, employees, telephone numbers, Laws, rules and regulations, Petitions, Government glossary News.	Business information Addresses, opening hours, employees, telephone numbers, Laws, rules and regulations	Knowledge base (static intranet) Knowledge management (LAN)
Interaction Phase	Downloading forms on Websites Submitting forms Online help with filling in forms (permits, birth / death certificates) Intake processes for permits etc. E-mail, Newsletters, Discussion groups (e-democracy), Polls and questionnaires, Personalized web pages, Notification	Downloading forms on websites Submitting forms Online help with filling in forms (permits) Intake processes for permits etc. E-mail notification	E-mail Interactive knowledge databases Complaint handling tools
Transaction Phase	License applications /renewals Renewing car tags, vehicle registration, Personal accounts (mytax, myfines, mylicenses etc.) Payment of (property) taxes Payment of tickets and fines Paying utility bills Registering and voting online	License applications and renewals via website Payment of taxes Procurement	Inter-governmental transactions
Transformation Phase	Personalized website with integrated personal account for all services	Personalized website with integrated business account for all services	Database integration

Transformation Phase

The *fourth phase* is the transformation phase in which all information systems are integrated and the public can get G2C and G2B services at one (virtual) counter. One single point of contact for all services is the ultimate goal. The complex aspect in reaching this goal is mainly on the internal side, e.g. the necessity to drastically change culture, processes and responsibilities within the government institution (G2G). Government employees in different departments have to work together in a smooth and seamless way. In this phase cost savings, efficiency and customer satisfaction are reaching highest possible levels.

3.4.3 Vikas Nath Approach [17]

Vikas Nath has classified e-Governance models into the following categories:

- Broadcasting / Wider-Dissemination Model
- Critical Flow Model
- Comparative Analysis Model
- E-Advocacy/ Lobbying and Pressure Group Model
- Interactive- Service Model

1. Broadcasting Model

The model is based on broadcasting or dissemination of useful governance information, which already exists in the public domain into the wider public domain through the use of ICT and convergent media. The utility of this model is that a more informed citizenry is better able to benefit from governance related services that are available for them.

2. Critical Flow Model

The model is based on broadcasting or dissemination information of 'critical' value (which by its very nature will not be disclosed by those involved with bad governance practices) to targeted audience using ICT and convergent media. Targeted audience may include media, opposition parties, judicial bench, independent investigators or the wider public domain itself.

3. Comparative Analysis Model

Comparative Knowledge Model is one of the least-used but a highly significant model for developing country which is now gradually gaining acceptance. The model can be used for empowering people by matching cases of bad governance with those of good governance, and then analyzing the different aspects of bad governance and its impact on the people.

4. E-advocacy Model

E-Advocacy / Mobilization and Lobbying Model is one of the most frequently used Digital Governance model and has often come to the aid of the global civil society to impact on global decision-making processes. The strength of this model is in its diversity of the virtual community, and the ideas, expertise and resources accumulated through this virtual form of networking.

5. Interactive Model

Interactive-Service model is a consolidation of the earlier presented digital governance models and opens up avenues for direct participation of individuals in the governance processes. Fundamentally, ICT have the potential to bring in every individual in a digital network and enable interactive (two-way) flow of information among them.

3.5 Challenges of e-Governance

There are numerous potential barriers [22] related to the implementation of e-Governance. Fahnbulleh [25] identified the following as key barriers:

- Concerns about inadequate security and privacy of data
- Unequal access to computer technology by citizens
- High initial costs of setting up an e-Governance solution
- Resistance to change

Different platforms identify these challenges in different manners. The main challenges identified are trust, resistance to change, digital divide, cost and privacy and security concerns. It should be remembered that they do not exist in isolation. One challenge can have an effect on one or more of the other categories. For example, resistance to change might be influenced by a lack of trust, or the digital divide can be further widened because of inadequate funding.

3.5.1 Trust

Trust can be defined along two dimensions: as an assessment of a current situation, or as an innate personality trait or predisposition. Trust in itself varies with the individual and the situation. Issues pertaining to government can stimulate strong feelings of trust or mistrust in different constituents. The implementation of public administration functions via e-Governance requires the presence of two levels of trust. The first is that the user must be confident, comfortable and trusting of the tool or technology with which they will interact.

The second dimension of trust pertains to trust of the government. If a constituent has limited trust in either the technology or the government, it hampers their use of e-Governance systems.

Trust is an important recurring theme in user decision making. More specifically, trust has been examined in the context of electronic commerce and it is a significant factor affecting an individual's purchase decision. By extension, an individual constituent that has previously not established trust in the e-commerce domain can transfer that lack of trust to other areas, such as government.

3.5.2 Resistance to Change

The innovation diffusion theory states that over time an innovation will diffuse through a population, and the rate of adoption will vary between those who adopt early—referred to as “early adopters”—and to those who adopt the innovation much later, referred to as “laggards”. The varying rates of adoption indicate that some users are more resistant to accepting the innovation which, in this case, is e-Governance.

The resistance to change phenomenon can explain much of the hesitation that occurs on the part of constituents in moving from a paper-based to a Web-based system for interacting with government. Income, age, and education are all contributing factors that can result in resistance to the use of e-Governance initiatives. Further, innate personal characteristics, such as dogmatism, can work to increase an individual's resistance to change. If there is a great preference to maintain the existing status quo, then there is a greater likelihood that resistance to new methods of operation will persist. Long-term employees may be particularly susceptible to this problem, since they may have completed tasks the same way for many years.

Citizens, employees and businesses can all have their biases with respect to how transactions should be processed. However, government entities and public policy administrators cannot ignore the changes that occur as a result of the implementation of information and communication technology (ICT). In the early 1990s Freeman identified the important role that ICT would have in shaping public policy, and cautioned both rich and poor governments about neglecting its significance. Education about the value of the new systems is one step toward reducing some of the existing resistance.

3.5.3 Digital Divide

The digital divide refers to the separation that exists between individuals, communities, and businesses that have access to information technology and those that do not have such access [40, 8]. Social, economic, infrastructural and ethno-linguistic indicators provide explanations for the presence of the digital divide. Further the presence of the digital divide indicates that a community might not be fully equipped with the tools or knowledge to benefit from the implementation of e-Governance projects.

Many non-profit and community based organizations (CBO) provide valuable public services to various communities. Some of these organizations work very closely with government agencies via grant requests and information sharing. With the use of e-Governance for the dissemination of critical information, many of the smaller agencies that lack the necessary infrastructure may not reap the benefits available through the Web. In fact, many of the smaller CBOs succumb to the “organizational divide” where they lack the means to remain informed and current with the new technology. The limited access to information can indeed impede an organization’s willingness to support the adoption of new e- governance projects in the public domain.

Economic poverty is closely related to limited information technology resources. An individual living at or below the poverty level is less likely to have a personal computer at home and may need to rely on work or public domains (such as public libraries) to provide access to e- governance and other online services. Limited availability of the necessary information technology infrastructure can serve as a great deterrent to the adoption of any Web-based initiatives. As the digital divide narrows, broader adoption of e- governance services in the public domain becomes possible.

3.5.4 Cost

Cost is generally a prohibitive factor in the implementation of information technology, particularly in the public sector where other projects and initiatives might have a higher priority than e-Governance. Elected officials responsible for allocation of funds may also be unwillingly to promote such projects where the returns are not always visible in the short term and utilization of the technology is not guaranteed. Typically costs associated with e-governance projects include: hardware, software, testing, training, migration to new system and maintenance. In the near future, cost will continue to be a significant challenge to extensive and comprehensive implementation of e-Governance projects for government.

3.5.5 Privacy and Security

With the implementation of e- governance projects, effective measures must be taken to protect sensitive personal information. A lack of clear security standards and protocols can limit the development of projects that contain sensitive information such as income, medical history, etc. Further, users must be confident that the Websites they visit and transactions they complete are safeguarded against theft, fraud and unauthorized access. A one size model cannot fit all consumers.

3.5.6 Issues for e-Governance Implementation

In the light of above discussions, demand (requirements) of the citizens and changing global scenario, there are certain issues which need attention [77].

Funding: This is the foremost issue in e-Governance initiatives. The projects that are part of the e-Governance initiatives need to be funded either through the Government sector or through the private sector. For the private sector to step into the funding activity their commercial interests needs to be ensured. The projects can be built either on BOO (Built Own Operate) or BOOT (Built Own Operate Transfer) basis. Also the Government interest of value addition in services also needs to be taken care of while transferring the services to private sector. Advertising, sharing of Government information etc could be a few revenue generators for the Government.

Change Management: The delivery of Government services through the electronic media including EDI, Internet and other IT based technologies would necessitate procedural and legal changes in the decision and delivery making processes. It demands fundamental changes in Government decision management. The employees need to be delegated more authority. De-layering of the decision-making levels leads to re-engineering and appropriate sizing of the decision-making machinery. These changes need not only be accepted by the Government and citizens but also be accepted by various interests groups like Employees unions. Under such circumstances bringing in a change will involve changing the mindsets of the people, and a complete reengineering process needs to be carried out for the same. This will involve training of the personnel at all levels, more so, at the lower rung of Government management organizations. There will also be a loss of vested interests and power amongst the legislature and the executive, which may lead, to resistance to change.

Authentication: Secured ways of transactions for the Government services are another issue of concern. The identity of citizens requesting services needs to be verified before they access or use the services. Here digital signature will play an important role in delivery of such services. But the infrastructure needed to support them is very expensive and requires constant maintenance. Hence a pertinent need still survives, compelling the authorities to ensure the authenticity in their transactions thereby gaining absolute trust and confidence of the citizen.

Interoperability: A major design issue for integrated service delivery sites is, how to capture data in a Web-based form and transfer it to an agency's systems for processing and sharing that information in a common format. In fact the interoperation of various state Governments, the various ministries within a state Government is a critical issue. Further how the various islands of automation will be brought together and built into one is another key issue of e-Governance.

Delivery of services: The ability of citizens to access these services is another major issue. Since the penetration of PCs and Internet is very low in the country, some framework needs to be worked out for delivery of the e-Services that would be accessible to the poorest of the poor. What will be the Government's network to deliver those services? Could we have something like a single stop shop of the Government? A proposed mechanism is delivery of the same through the Government Post Offices, for they already have the brick and mortar support and the most extensive network in the nation.

Standardization: Defining the standards for the various Government services is another issue that needs to be addressed. The standards need to be worked out not only for the technologies involved but also for issues like naming of websites to creating E-Mail addresses, capturing of biometric data etc.

Technology Issues: A number of organizations, both in the Centre and the States, have taken commendable initiatives to develop hardware and software platforms to address the challenges offered by e-Governance. At the central level in particular, the NIC and C-DAC, and a number of others are noteworthy. The e-Governance initiative would have to address these Technology Issues/Objectives by identifying the appropriate hardware platforms and software application packages for cost-effective delivery of public services. This knowledge repository should be widely available through appropriate Demo- Mechanisms. Offering a basket of these models to the State departments, both in the Center and the State, could be suitably customized as per location and work specific requirements.

Use of local languages: The access of information must be permitted in the language most comfortable to the public user, generally the local language. There already exist technologies such as GIST and language software by which transliteration from English into other languages have been attempted.

3.6 Initiatives of the Government of India [57]

A major initiative of the Government for ushering in e-Governance on national scale, called National e-Governance Plan (NeGP) was approved on 16 May 2006. The main objective of NeGP is to “make all government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realize the basic needs of the common man”.

Broadly NeGP consists of 31 Mission Mode Projects (MMPs) encompassing 11 central MMPs, 13 state MMPs and 7 integrated MMPs that span multiple backend Ministries/ departments. It also includes 8 program support components aimed at creating the right governance and institutional mechanisms, core infrastructure, policies & standards and the necessary legal framework for adoption of e-Governance in the country. It is implemented at the Central, state and Local Government levels. Major achievements of NeGP are as under.

Under NeGP, Government had approved a Scheme for facilitating establishment of more than 100,000 broadband Internet-enabled Common Service Centres (CSCs) in rural areas of the country at a total cost of Rs. 1649 crore. It is being implemented under Public Private Partnership mode. As of 30th April, 2012, more than 88000 CSCs have been operationalised. Under NeGP, Government had approved the Scheme for establishing State Wide Area Networks (SWANs) across the country in 29 States/ 6 UTs at a total outlay of Rs. 3,334 crore. Under this Scheme, it is envisaged to provide secured Network from State Headquarters up to the Block level with a minimum bandwidth capacity of 2 Mbps. As of April 2012 SWANs in 30 States/ UTs have been rolled out, while in other States/ UTs they are expected to be rolled out by March 2013.

State Data Centre (SDC) has been identified as one of the important elements of the core infrastructure for supporting e-Governance initiatives under NEGP. The Government has approved the scheme in January 2008 at an estimated outlay of Rs. 1623.20 crore to cover 28 States and 6 UTs across the country. So far the SDCs in 16 State/UTs have been set up.

In order to provide a mechanism for adequate capacity building and training for end user, a Capacity Building Scheme at an outlay of Rs. 313 crore has been approved in January 2008. This envisions establishment of institutional framework for State Level Strategic decision-making including setting-up of State e-Governance Mission Teams (SeMTs). A Capacity Building Management Cell (CBMC) has been set up in DeitY for overall coordination and implementation of Capacity Building Scheme.

To provide transparent, speedier and efficient Justice, the Government has initiated several steps to transform the Indian Judiciary in about 13,000 District & Subordinate courts across the country.

The last decade represented an era of strong growth in the domain of e- governance. However, issues related to security continue to be a challenge. As more information is collected, additional vulnerabilities are exposed. Indeed, security is poised to be a recurring problem in this domain as the growth in this area continues to take place. Great strides have been made in recent years and new practices and procedures are in the developmental stage.

Besides security, universal access to government services will also be an important issue in the future. In particular, individuals with special needs, seniors and persons with disabilities will be given strong focus. Full e-Governance access to persons with a disability is yet to be achieved. As the world's population ages, senior citizens will present unique needs and will request services that must be delivered in a manner that is readily accessible to them.

3.7 Summary

The strategic and contemporary importance of e-Governance has been recognised across the world. The emergence and use of ICT is clearly one of the major potential solutions in the desire to achieve improved governance. The use of e-Governance services to improve public administration functions will continue to have a strong impact on the operation of Central and State governments in India and the rest of the world. e-Governance can also serve as a catalyst for the radical redesign of governmental organizations and agencies. There are numerous benefits [28] and challenges that can result from these changes. The following major challenges will remain in the next decade: trust building in e-Governance, ICT management, and privacy and security.

Designing and implementing more effective approaches and plans for securing e-Governance projects is an important issue, because, the governmental information is usually highly

sensitive. Thus e-Governance projects cannot be planned from outside. A holistic approach has to be adopted in order to understand the needs of the citizens, the capabilities of the government organisations, their processes and structures, based on these points the technology based solution would have to be devised. Furthermore, security has an important role in trust formation of citizens and their adoption of e-Governance. Security for e-Governance system also is to be designed and managed from a holistic point of view.

The following chapters identify the information security requirements for e-Governance services, and suggest appropriate controls to meet the same.

e-Governance Security Requirement

4.1 Introduction

The nation's IT infrastructure has undergone a dramatic transformation over the last decade. Today's computing system comprises a broad range of processors, communication networks and information repositories. Because of the tremendous productivity gains and new capabilities enabled by these network systems, they have been incorporated into vast number of civilian applications. They have also become part of the nation's critical infrastructure – including communications, finance, law enforcement and defence.

Due to the ubiquitous nature of these network systems, they are increasingly subject to attacks, misuse and abuse. Some common types of attacks are Eavesdropping, Data Modification, Identity Spoofing (IP Address Spoofing), Password-Based Attacks, Denial-of-Service Attacks, Man-in-the-Middle Attacks, Compromised-Key Attacks, Sniffer Attacks, and Application-Layer Attacks. Examples of abuse include cyber bullying, cyber baiting and social network profile abuses. Computing systems are vulnerable to these threats due to technical (e.g. lack of security controls) and economic (e.g. shortage of funds for investing in security tools) factors. Today it is possible for the malicious agent to penetrate millions of computers in a matter of minutes, exploiting those machines to attack the nation's critical infrastructure, penetrate sensitive systems or steal valuable data. For example, recently the Flame computer virus not only stole large quantities of information from various Iranian government agencies, but apparently even disrupted its oil exports by shutting down oil terminals. The growth in the number of attacks matches the tremendous growth in connectivity. Internet users in the country grew from 1.4 million in 1999 to over 100 million by 2011. The cyber incidents handled by CERT-In increased from 254 in the year 2005 to over 13000 in the year 2011. Dealing with these attacks has become increasingly complex and sophisticated. The short term patches and fixtures that are deployed today to plug the holes/vulnerabilities can be useful in response to isolated vulnerabilities. But they do not adequately address the core problem. A comprehensive risk management programme needs to be implemented in order to identify and address e-Governance security requirements.

The CISA Review Manual 2006 provides the following definition of risk management: “*Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.*”

Risk is the likelihood that something bad will happen that causes harm to an asset (or the loss of the asset) [65]. A **vulnerability** is a weakness that could be used to endanger or cause harm to an asset. A **threat** [24] is anything (man-made or act of nature) that has the potential to cause harm. The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (loss of income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called *residual risk*.

The *process* of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. Also, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected. Several risk management standards have been developed in various organizations like the Project Management Institute, the National Institute of Science and Technology, actuarial societies, and ISO.

Strategies to manage risk typically include transferring the risk to another party, avoiding the risk, reducing the negative effect or probability of the risk, or even accepting some or all of the potential or actual consequences of a particular risk. Thus, for any given risk, Executive Management can choose to **accept the risk** based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to **mitigate the risk** by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be **transferred** to another business by buying insurance or out-sourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to **deny the risk**.

4.2 Security Controls

When Management chooses to mitigate a risk, they do so by implementing one or more of three different types of security controls [12] in the context of security management.

4.2.1 Administrative controls

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards [2] and guidelines that must be followed – the Payment Card Industry (PCI) Data Security Standard required by Visa and Master Card is such an example. Other examples of administrative controls include the corporate information security policy, password policy, HR policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls.

4.2.2 Logical controls

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

4.2.3 Physical controls

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

4.2.4 Defence-in-depth

Information security must protect information throughout the life span of the information, from the initial creation of the information through to the final disposal of the information. Information must be protected while in motion and while at rest. During its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways that information and information systems can be threatened. To fully protect information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defence-in-depth (Figure 4.1). The strength of any system is no greater than its weakest link. Using a defence-in-depth strategy, should one defensive measure fail, there are other defensive measures in place that continue to provide protection.

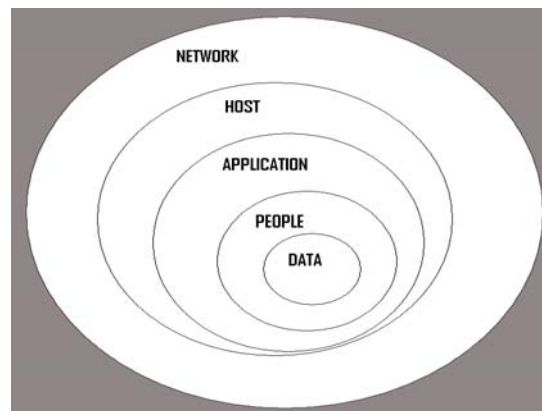


Figure 4.1: Defence-in-depth

A combination of administrative, logical, and physical controls can be used to form the basis upon which to build a defence-in-depth strategy. With this approach, defence-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defence-in-depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people the next outer layer of the onion, and network security, host-based security and application security forming the outermost layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defence-in-depth strategy.

4.3 Security Classification for information

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to put in place the policy and commitment by senior management and identify the roles of users for classification data and implementing the security level according the classification. This policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Legal and regulatory requirements are also important considerations when classifying information.

The type of information security classification labels selected and used will depend on the nature of the organisation, with examples being:

- In the business sector, labels such as: **Public, Sensitive, Private, Confidential.**
- In the government sector, labels such as: **Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret, Top Secret.**

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification of a particular information asset should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place and being enforced effectively.

4.4 Information Security Threats and Security Requirements

Examining the overall process, beginning with the consumer and ending with the e-Governance server, helps in identifying e-Governance security requirements [55]. The assets that must be

protected to ensure secure e-Governance include client computers (including mobile devices), the messages traveling on the communication channel, and the Web and e-Governance servers – including any hardware attached to the servers. This section looks at various kinds of threats and the security requirements that these threats attempt to breach.

4.4.1 Client End Threats

Until the introduction of executable Web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. But, the widespread use of active content has changed this perception.

a. Active Content

Active Contents like Java applets, ActiveX controls, JavaScript, and VBScript refer to programs that are embedded transparently in Web pages and that cause action to occur. Active content can display moving graphics, download and play audio, or implement Web-based spreadsheet programs. Active content is used in many cases to compute the total invoice amount, including sales tax, handling, and shipping costs. Embedding active content to Web pages involved in e-Governance increases security risks to client systems, thereby putting onus on concerned service provider or owner of such E-Gov service to put in place appropriate security mechanisms. Malicious programs delivered quietly via Web pages could reveal credit card numbers, usernames, and passwords that are frequently stored in special files called cookies. Malicious active content delivered by means of cookies can reveal the contents of client-side files or even destroy files stored on client computers.

b. Malicious Codes

Computer viruses, worms and Trojan Horses are examples of malicious code. The malware trends indicate that malicious code is becoming more sophisticated and rather than creating destruction (such as Blaster worm, Mydoom etc.) more purpose-oriented malware are being created by cyber criminals. Recent malware such as ZeuS and Spyeye are very stealthy and steal specific information of users to conduct financial frauds. Worms such as Conficker that transpired in late 2009 propagated world-wide and millions of systems are still infected by this worm. Such malware can download more updated malicious code on to target systems.

People are aware but may not be prepared to deal with such threats since prevention of malware infection indeed requires reasonable caution and discipline by the users.

c. Server-side masquerading

Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the Internet but instead reaches another computer that claims to be the desired one, the user has been spoofed.

d. Unauthorized usage of the client machine

If a client machine or mobile device is logged to the server but remain idle for a long period of time, then it may become the victim of unauthorized usage by intruders.

4.4.2 Communication Channel Threats

The Internet serves as the electronic chain linking a consumer (client) to the e-Governance server. Messages on the Internet travel a random path from a source node to a destination node. It is impossible to guarantee that every computer on the Internet through which messages pass is safe, secure, and non-hostile.

a. Confidentiality Threats

Confidentiality is the prevention of unauthorized information disclosure. Use of internet definitely poses confidentiality threats to the messages sent.

b. Integrity Threats

An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Unauthorized changes and defacing of web-pages may put any e-Governance project into jeopardy.

c. Availability Threats

The purpose of availability threats, also known as delay or denial of service threats, is to disrupt normal computer processing or to deny processing entirely. Slowing any Internet service will detract citizens from using e-Governance services. Figures 4.2 (a), (b), (c), and (d) show the no. of Indian websites defaced during 2006-2011[42, 43, 44, 45]. Defacement of websites is one of the commonest techniques of breaching availability of information.

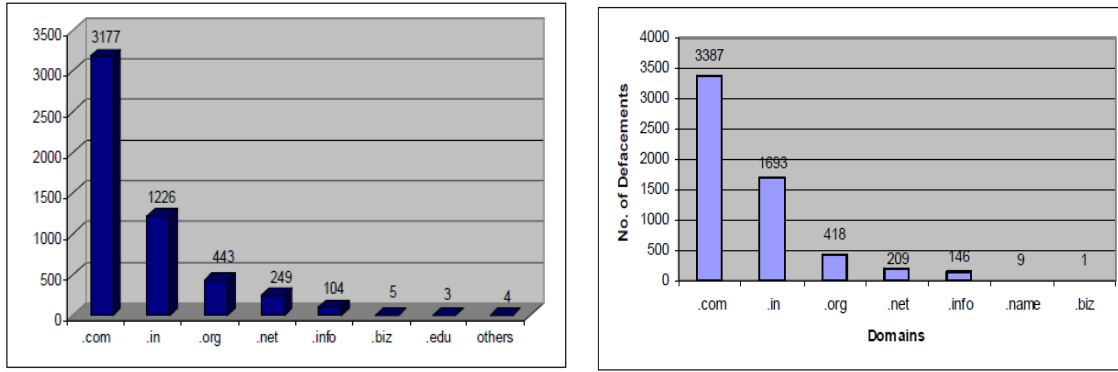


Figure 4.2(a): Indian websites defaced during 2006 and 2007, respectively

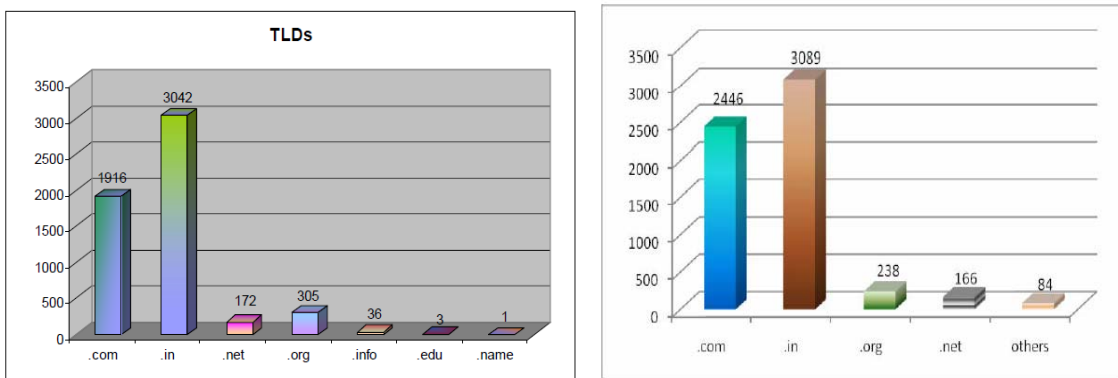


Figure 4.2(b): Indian websites defaced during 2008 and 2009, respectively

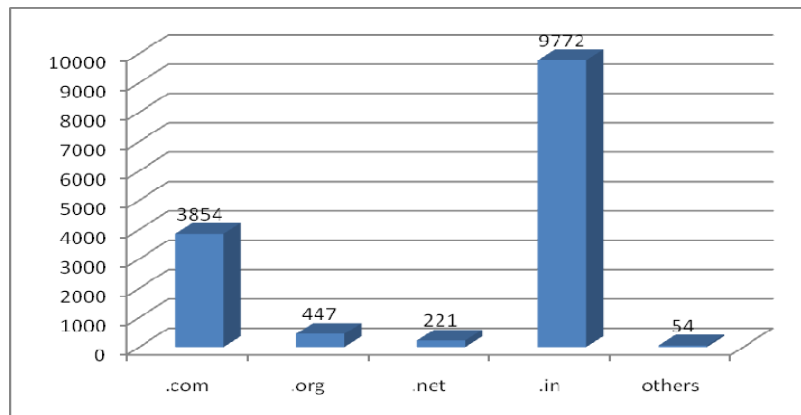


Figure 4.2(c): Indian websites defaced during 2010

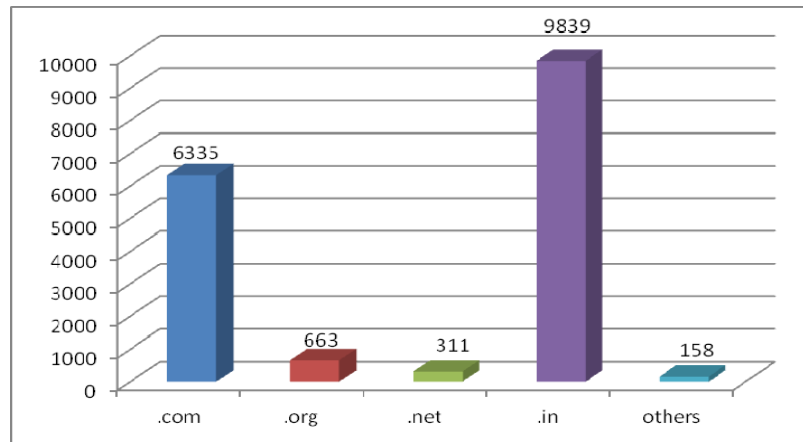


Figure 4.2(d): Indian websites defaced during 2011

4.4.3 Server End Threats

The server is the third link in the client-Internet-server trio embodying the e-Governance path between the citizen and the government. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

a. Web Server Threats

Web server software is designed to deliver Web pages by responding to Hyper-Text Transfer Protocol (HTTP) requests. While Web server software is not inherently high-risk, it has been designed with Web service and convenience as the main design goals. The more complex the software, the higher is the probability that it contains coding errors (bugs) and security holes.

b. e-Governance Server Threats

The e-Governance server, along with the Web server, responds to requests from Web browsers through the HTTP protocol and Common Gateway Interface (CGI) scripts. Several pieces of software comprise the e-Governance server software suite, including possibly an File Transfer Protocol (FTP) server, a mail server, a remote login server, and operating systems on host machines. Each of this software can have security holes and bugs.

c. Database Threats

e-Governance systems store huge amount of user data and retrieve information from databases connected to the Web server. Besides government information, databases connected to the Web contain critical and private information that could irreparably damage an enterprise or citizen if it were disclosed or altered. Some databases store username/password pairs in a non-secure way. If

someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.

d. Common Gateway Interface Threats

A CGI implements the transfer of information from a Web server to another program, such as a database program. CGI and the programs to which they transfer data provide active content to web pages. Because CGIs are programs, they present a security threat if misused. Just like Web servers, CGI scripts can be set up to run with their privileges set to high – unconstrained. Defective or malicious CGIs with free access to system resources are capable of disabling the system, calling privileged (and dangerous) base system programs that delete files, or viewing confidential customer information, including usernames and passwords.

e. Password hacking

The simplest attack against a password-based system is to guess passwords. Guessing of passwords require that access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.

f. Application server threats

e-Governance system application server contains the whole business logic of the system. One simplest way to demolish the total system is to attack the application server. Sometime the application servers store username and password in a non secure way. If someone can get the information then he or she can easily intrude to the system.

4.4.4 Insider Attacks

Some potential threat agents are users, e-Governance service operators and insiders for whom system authorities have some responsibilities and can exercise some control. These include:

I. Legitimate users of e-Governance services

Legitimate users may seek to misuse or damage e-Governance service provision. Such individuals may possess, or have access to, significant technical resources and skills with a strong motivation to compromise the services- frequently for financial gain. Some users may unintentionally damage e-Governance services. This may arise due to genuine mistake or non-intuitive service design. Such individuals do not intend to undermine the service provision but

nevertheless cause significant disruption. A legitimate user may collude with an e-Governance service and commit fraud or gain access to protected information.

II. Insiders

Insiders or e-Governance service operator or their representatives who are responsible for the provision or operation of e-Governance services may seek to exploit their privileged position. This group may include government employees, their agents or employees of outside organizations contributing to e-Governance services. Such individuals may possess significant resources and technical skills in addition to privileged access rights. Their motivation is likely to be fraud or personal dissatisfaction.

4.5 Security Postures to Support Data Characteristics and Access

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

For over twenty years information security has held that three key concepts form the core principles of information security: confidentiality, integrity and availability. These are known as the CIA Triad.

Confidentiality

Information that is considered to be confidential in nature must only be accessed, used, copied, or disclosed by persons who have been authorized to access, use, copy, or disclose the information, and then only when there is a genuine need to access, use, copy or disclose the information. A breach of confidentiality occurs when information that is considered to be confidential in nature has been, or may have been, accessed, used, copied, or disclosed to, or by, someone who was not authorized to have access to the information.

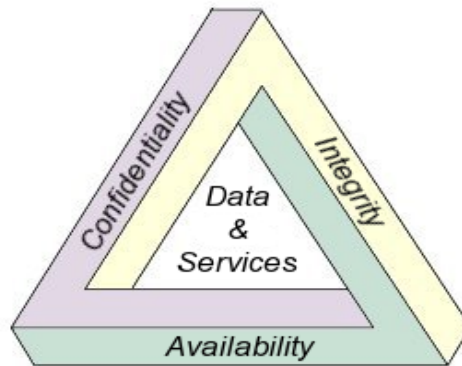


Figure 4.3: CIA Triad

Integrity

In information security, integrity means that data can not be created, changed, or deleted without authorization. It also means that data stored in one part of a database system is in agreement with other related data stored in another part of the database system (or another system). For example: a loss of integrity can occur when a database system is not properly shut down before maintenance is performed or the database server suddenly loses electrical power. A loss of integrity occurs when an employee accidentally, or with malicious intent, deletes important data files. A loss of integrity can occur if a computer virus is released onto the computer. A loss of integrity can occur when an on-line shopper is able to change the price of the product they are purchasing.

Availability

The concept of availability means that information, the computing systems used to process information, and the security controls used to protect information are all available and functioning correctly when information is needed. The opposite of availability is Denial of Service (DoS).

In addition to CIA, authenticity and non-repudiation requirements should also be catered to in an e-Governance scenario.

Authenticity

In computing, e-Business, and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine (i.e. they have not been forged or fabricated.)

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction can not deny having received a transaction nor can the other party deny having sent a transaction.

Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation. Digital signatures, a form of electronic signatures, are created and verified using Public Key Cryptography that is based on the concept of a key pair generated by a mathematical algorithm, the public and private keys. In India the Information Technology Act, 2008 provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents. The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users. The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the Root Certifying Authority of India (RCAI). The CCA also maintains the National Repository of Digital Certificates (NRDC), which contains all the certificates issued by all the CAs in the country.

There are four classes of digital signature certificates. They are as follows:

Class 0 Certificate: This certificate shall be issued only for demonstration/ test purposes.

Class 1 Certificate: Class 1 certificates shall be issued to individuals/private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.

Class 2 Certificate: These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.

Class 3 Certificate: This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.

4.5.1 Model-based Data location & Security Requirement Analysis of e-Governance Applications

e-Governance applications handle sensitive data of the government and public. The security requirements of the data are different for different applications. To implement data security, the security requirements along with the location of the data is to be considered. The security parameters to be considered are: Confidentiality(C), Integrity (I), Availability (A), Authentication (Au), and Non – Repudiation (Nr) [51].

4.5.1.1 Broadcasting Model

The model [17] is based on broadcasting or dissemination of useful governance information which already exists in the public domain into the wider public domain through the use of ICT and convergent media. The utility of this model is that a more informed citizenry is better able to benefit from governance related services that are available for them. Table 4.1 defines security requirements of the model according to different data locations.

Table 4.1: Security requirements of Broadcasting model

Data Location	Security Aspect	Threats	Vulnerabilities
Data in Store	Integrity	Encryption cracking	Using the same key for a prolonged period of time
	Availability	- System failure (Unavailability of information system) - Corruption / loss or damage of back up media	- Inadequate back up facilities - Non adherence to back up policy
	Authentication	Brute force attack (Exhaustive search / trying all possible outcomes)	- No Password - Minimum length of the password / Password complexity has not been enforced
Data in Process	Integrity	- Loss of decryption keys - Encryption cracking	- Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time
	Availability	- System failure (Unavailability of information system) - Corruption / loss or damage of back up media	- Inadequate back up facilities - Non adherence to back up policy
	Authentication	- Theft of credentials - Brute force attack	- No Password - Minimum length of the password has not been enforced - Password is guessable

Data Location	Security Aspect	Threats	Vulnerabilities
	Data validation	▪ Cross-site scripting ▪ Query string manipulation	▪ Using application-only filters for malicious input ▪ Using non-validated input used to generate SQL queries Relying on client side validation
Data in Transit	Integrity	▪ Encryption cracking	▪ Using the same key for a prolonged period of time
	Authentication	▪ Brute force attack	▪ No Password ▪ Minimum length of the password has not been enforced ▪ Password is guessable
	Sensitive data	▪ Network eavesdropping	▪ Passing sensitive data in clear text over network
Data in Destination	Integrity	▪ Encryption cracking	▪ Using the same key for a prolonged period of time

4.5.1.2 Critical Flow Model

The model [19] is based on broadcasting or dissemination information of “critical” value (which by its very nature will not be disclosed by those involved with bad governance practices) to targeted audience using ICT and convergent media. Targeted audience may include media, opposition parties, judicial bench, independent investigators or the wider public domain itself.

Table 4.2: Security requirements of Critical Flow model

Data Location	Security Aspect	Threats	Vulnerabilities
Data in Store	Confidentiality	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Availability	▪ System failure (Unavailability of information system)	▪ Absence of back up policy ▪ Inadequate back up facilities
	Authentication	▪ Brute force attack ▪ Impersonation ▪ Inability to identify actual user	▪ No Password ▪ Minimum length of the password has not been enforced ▪ Password is guessable ▪ Password sharing among the peer user

Data Location	Security Aspect	Threats	Vulnerabilities
	Non-Repudiation	- Denial of service attacks - Misuse of privileges	- Lack of monitoring of services and activities - Inadequacy in contract documentation (service definition, dos & don'ts and other important processes)
Data in Process	Confidentiality	Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small
	Integrity	Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small
	Availability	- System failure (Unavailability of information system) - Unsuccessful recovery - Corruption / loss or damage of back up media	- Absence of back up policy - Inadequate back up facilities - Non adherence to back up policy
	Authentication	- Brute force attack - Impersonation	- Minimum length and complexity of the password has not been enforced - Password is guessable - Password sharing among the peer user
	Data validation	- Form field manipulation - Cookie manipulation - HTTP header manipulation	- Using non-validated input used to generate SQL queries - Relying on client side validation - Failing to validate input from all sources including cookies, query string parameters, HTTP headers, databases and network resources
Data in Transit	Confidentiality	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Integrity	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Authentication	- Brute force attack - Impersonation	- Minimum length and complexity of the password has not been enforced - Password is guessable - Password sharing among the peer user
	Sensitive data	Network eavesdropping	Passing sensitive data in clear text over network

Data Location	Security Aspect	Threats	Vulnerabilities
Data in Destination	Confidentiality	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Integrity	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Authentication	Impersonation	- Minimum length and complexity of the password has not been enforced - Password is guessable
	Non-Repudiation	- Denial of service attacks - Misuse of privileges	- Lack of monitoring of services and activities - Inadequacy in contract documentation (service definition, dos & don'ts and other important processes)

4.5.1.3 Comparative Analysis Model

Comparative Analysis Model [18] is one of the least-used but a highly significant model for developing country which is now gradually gaining acceptance. The model can be used for empowering people by matching cases of bad governance with those of good governance, and then analyzing the different aspects of bad governance and its impact on the people.

Table 4.3: Security requirements of Comparative Analysis model

Data Location	Security Aspect	Threats	Vulnerabilities
Data in Store	Integrity	Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time
	Availability	- System failure (Unavailability of information system) - Unsuccessful recovery - Corruption / loss or damage of back up media	- Absence of back up policy - Inadequate back up facilities - Non adherence to back up policy - No back up copy kept off-site - Backup media unusable
	Authentication	Theft of credentials	Use of weak cipher or hash to make password non readable

Data Location	Security Aspect	Threats	Vulnerabilities
Data in Process	Integrity	Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time
	Availability	- System failure (Unavailability of information system) - Unsuccessful recovery - Corruption / loss or damage of back up media	- Absence of back up policy - Inadequate back up facilities - Non adherence to back up policy - No back up copy kept off-site - Backup media unusable
	Authentication	- Theft of credentials - Brute force attack	Use of weak cipher or hash to make password non readable
	Data validation	Form field manipulation	Using input file names, URLs or user names for security decisions
Data in Transit	Integrity	Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time
	Authentication	- Theft of credentials - Brute force attack	Use of weak cipher or hash to make password non readable
	Sensitive data	Network eavesdropping	Passing sensitive data in clear text over network
Data in Destination	Integrity	Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time
	Availability	- System failure (Unavailability of information system) - Unsuccessful recovery - Corruption / loss or damage of back up media	- Absence of back up policy - Inadequate back up facilities - Non adherence to back up policy - No back up copy kept off-site - Backup media unusable
	Authentication	Brute force attack	- Minimum length and complexity of the password has not been enforced - Password is guessable

4.5.1.4 E-Advocacy Model

E-Advocacy / Mobilization and Lobbying Model [20] is one of the most frequently used Digital Governance model and has often come to the aid of the global civil society to impact on global decision-making processes. The strength of this model is in its diversity of the virtual community, and the ideas, expertise and resources accumulated through this virtual form of networking.

Table 4.4: Security requirements of E-Advocacy model

Data Location	Security Aspect	Threats	Vulnerabilities
Data in Store	Integrity	Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time
	Availability	- System failure (Unavailability of information system) - Unsuccessful recovery - Corruption / loss or damage of back up media	- Absence of back up policy - Inadequate back up facilities - Non adherence to back up policy - Corruption of Back up media
	Authentication	- Brute force attack - Impersonation - Inability to identify actual user	- Complexity of the password is not enforced - Use of weak cipher or hash to make password non readable
Data in Process	Integrity	Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time
	Availability	- System failure (Unavailability of information system) - Unsuccessful recovery - Corruption / loss or damage of back up media	- Absence of back up policy - Inadequate back up facilities - Non adherence to back up policy
	Authentication	- Brute force attack - Impersonation - Inability to identify actual user	- Complexity of the password is not enforced - Use of weak cipher or hash to make password non readable
	Data validation	- Cookie manipulation - HTTP header manipulation	Failing to validate input from all sources including cookies, query string parameters, HTTP headers, databases and network resources
Data in Transit	Integrity	Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time
	Availability	System failure (Unavailability of information system)	Non adherence to back up policy
	Sensitive data	- Network eavesdropping - Information disclosure	- Storing secrets when it is not needed - Storing secrets in clear text - Passing sensitive data in clear text over network

Data Location	Security Aspect	Threats	Vulnerabilities
Data in Destination	Integrity	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Availability	System failure (Unavailability of information system)	Non adherence to back up policy
	Authentication	- Theft of credentials - Inability to identify actual user	- Complexity of the password is not enforced - Use of weak cipher or hash to make password non readable

4.5.1.5 Interactive-Service Model

Interactive-Service model [21] is a consolidation of the earlier presented digital governance models and opens up avenues for direct participation of individuals in the governance processes. Fundamentally, ICT have the potential to bring in every individual in a digital network and enable interactive (two-way) flow of information among them.

Table 4.5: Security requirements of Interactive Service model

Data Location	Security Aspect	Threats	Vulnerabilities
Data in Store	Confidentiality	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Integrity	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Availability	- System failure (Unavailability of information system) - Unsuccessful recovery / Corruption / loss or damage of back up media	- Absence of back up policy - Inadequate back up facilities - Non adherence to back up policy - No back up copy kept off-site

Data Location	Security Aspect	Threats	Vulnerabilities
	Authentication	- Impersonation - Inability to identify actual user	- Password sharing among the peer user - Complexity of the password is not enforced - Use of weak cipher or hash to make password non readable
	Non-Repudiation	Denial of service attacks	Inadequacy in contract documentation (service definition, dos & don'ts and other important processes)
Data in Process	Confidentiality	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Integrity	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Availability	System failure (Unavailability of information system)	- Absence of back up policy - Inadequate back up facilities
	Authentication	- Theft of credentials - Brute force attack	- Complexity of the password is not enforced - Use of weak cipher or hash to make password non readable
	Non-Repudiation	Misuse of privileges	Lack of monitoring of services and activities
Data Transit	Confidentiality	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Integrity	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Authentication	Theft of credentials	- No Password - Complexity of the password is not enforced

Data Location	Security Aspect	Threats	Vulnerabilities
	Sensitive data	- Network eavesdropping - Information disclosure	- Storing secrets when it is not needed - Storing secrets in clear text - Passing sensitive data in clear text over network
Data in Destination	Confidentiality	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Integrity	- Loss of decryption keys - Encryption cracking	- Failing to secure encryption keys - Using the wrong algorithm or a key size that is too small - Using the same key for a prolonged period of time - Distributing keys in an insecure manner
	Authentication	- Brute force attack - Inability to identify actual user	- Minimum length of the password has not been enforced - Password is guessable - Password sharing among the peer user - Use of weak cipher or hash to make password non readable
	Authentication	- Brute force attack - Inability to identify actual user	- Minimum length of the password has not been enforced - Password is guessable - Password sharing among the peer user - Use of weak cipher or hash to make password non readable
	Non-Repudiation	- Denial of service attacks - Misuse of privileges	- Lack of monitoring of services and activities - Inadequacy in contract documentation (service definition, dos & don'ts and other important processes)

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected - the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built starts with identification and authentication.

Identification is an assertion of who someone is or what something is. If a person makes the statement “Hello, my name is Vipin Yadav” he is making a claim of who he is. However, the claim may or may not be true. Before Vipin Yadav can be granted access to protected information it will be necessary to verify that the person claiming to be Vipin Yadav really is Vipin Yadav.

Authentication is the act of verifying a claim of identity. When Vipin Yadav goes into a bank to make a withdrawal, he tells the bank teller he is Vipin Yadav (a claim of identity). The bank teller asks to see a photo ID, so he hands the teller his driver’s license. The bank teller checks the license to make sure it has Vipin Yadav printed on it and compares the photograph on the license against the person claiming to be Vipin Yadav. If the photo and name match the person, then the teller has authenticated that Vipin Yadav is who he claimed to be.

On computer systems in use today, *Username* is the most common form of identification and *Password* is the most common form of authentication. Usernames and passwords have served their purpose but in our modern world they are no longer adequate. Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (read, write, modify, append, delete, and execute). This is called authorization. Authorization to access information and other computing services begins with administrative policies and procedures. Policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies.

Different computing systems are equipped with different kinds of access control mechanisms; some may offer a choice of different access control mechanisms. The access control mechanism that a system offers will be based upon one of three approaches (detailed in Section 6.2 of Chapter 6) to access control or it may be derived from a combination of the three approaches.

The *non-discretionary* approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individual’s function (role) in the organization or the tasks the individual must perform. The *discretionary* approach gives the creator or owner of the information resource the ability to control access to

those resources. In the *mandatory* access control approach, access is granted or denied bases upon the security classification assigned to the information resource. Examples of common access control mechanisms in use today include Role-based access controls available in many advanced Database Management Systems, simple file permissions provided in the UNIX and Windows operating systems, Group Policy Objects provided in Windows network systems, Kerberos, RADIUS, TACACS, and the simple access lists used in firewalls and routers.

To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held accountable for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of audit trail. Access requirements of data are identified for different users and also for different models described above. Access modes considered are read, write, modify, append, delete, and execute.

4.5.2 e-Governance application user's access requirements

Tables 4.6 – 4.10 provide the access requirements of users for different models of e-Governance applications in G2C domain. The degree of the parameters of security requirements are to be identified on a case by case basis. The advantage of this approach is that the security analyst need not study each and every application separately. Rather, once the G2C application is classified into the specific model, the security requirements can be straight away inferred from this study. Standards of security may be written based on the e-Governance models; this will result in fewer human errors and bias.

Broadcasting / Wider-Dissemination Model

Table 4.6: Access requirements of Users for Broadcasting model

Users	Read	Write	Delete	Execute	Modify	Append
Database Manager	Y	Y	Y	Y	Y	Y
Developer	Y	Y	N	Y	N	Y
Implementation Officer	Y	N	N	Y	N	Y
Information Officer	Y	Y	Y	Y	Y	Y
Chief Information security Officer	Y	N	N	Y	N	Y
Officers and Employees	Y	N	N	Y	N	N
Agents	Y	N	N	Y	N	N
Public	Y	Y	N	Y	N	Y

Critical Flow Model**Table 4.7: Access requirements of Users for Critical Flow model**

Users	Read	Write	Delete	Execute	Modify	Append
Database Manager	Y	Y	Y	Y	Y	Y
Developer	Y	Y	N	Y	N	Y
Implementation Officer	Y	N	N	Y	N	Y
Information Officer	Y	Y	N	Y	N	Y
Chief Information security Officer	Y	N	N	Y	N	Y
Officers and Employees	Y	N	N	Y	N	N
Agents	Y	N	N	Y	N	N
Public	Y	N	N	Y	N	Y

Comparative Analysis Model**Table 4.8: Access requirements of Users for Comparative Analysis model**

Users	Read	Write	Delete	Execute	Modify	Append
Database Manager	Y	Y	Y	Y	Y	Y
Developer	Y	Y	N	Y	N	Y
Implementation Officer	Y	N	N	Y	N	Y
Information Officer	Y	Y	N	Y	N	Y
Chief Information security Officer	Y	N	N	Y	N	Y
Officers and Employees	Y	N	N	Y	N	N
Agents	Y	N	N	Y	N	N
Public	Y	N	N	Y	N	Y

E-Advocacy/ Lobbying and Pressure Group Model**Table 4.9: Access requirements of Users for E-Advocacy model**

Users	Read	Write	Delete	Execute	Modify	Append
Database Manager	Y	Y	Y	Y	Y	Y
Developer	Y	Y	Y	Y	Y	Y
Implementation Officer	Y	N	N	Y	N	Y
Information Officer	Y	Y	N	Y	N	Y
Chief Information security Officer	Y	N	N	Y	N	Y
Officers and Employees	Y	N	N	Y	N	N
Agents	Y	N	N	Y	N	N
Public	Y	Y	Y	Y	Y	Y

Interactive Service Model**Table 4.10: Access requirements of Users for Interactive Service model**

Users	Read	Write	Delete	Execute	Modify	Append
Database Manager	Y	Y	Y	Y	Y	Y
Developer	Y	Y	Y	Y	Y	Y
Implementation Officer	Y	N	N	Y	N	Y
Information Officer	Y	Y	Y	Y	Y	Y
Chief Information security Officer	Y	N	N	Y	N	Y
Officers and Employees	Y	N	N	Y	N	N
Agents	Y	N	N	Y	N	N
Public	Y	Y	N	Y	N	Y

4.6 A Structured Approach to Information Security Design

Technology components of good online security, such as encrypted email, secure socket layer (SSL) websites, and intranets/extranets all have a role to play in protecting valuable data. For security to be effective it must be designed as a whole and applied consistently across an organization and its IT infrastructure. In the case of security systems, the designer has to ensure that the system properties are preserved in the face of attacks. The steps to design security of a system is to model the system, identify the security properties to be preserved, model the adversary, and then ensure that the security properties are preserved under attacks. Detailed modeling of the system and identification of the required security properties are possible. But it is almost impossible to accurately model the adversaries and vulnerabilities of the system exploited by those adversaries. The result is that there is nothing called absolute security. Thus, to the designer, system security means: under given assumptions about the system, no attack of a given form will destroy specified properties. Therefore, system security in general and e-Governance security in particular is conceived as a process rather than a one-time developed product.

4.6.1 Security Management

e-Governance security covers of three distinguishable areas of environment; they are user environment, transport environment and ICT assets environment. Users can be internal or external, transport of information can be through private or public networks and the ICT assets can be tangible or intangible.

Important item of user environment is management of identities with access and interactions. Management of identities involves creation of digital identities or credentials for citizens, businesses and government officials. Conventionally, user names and passwords are used for management of identities of users. The e-Governance projects should have clear-cut password policies for creating and using passwords. Access management enables ICT systems to identify the valid users by matching passwords or other devices that carry the digital identity of the users. It also authorizes a user to perform only those tasks and transactions granted to the user.

The objective of interaction management system is to provide very important services of authentication, integrity, confidentiality, and non-repudiation. Authentication assures that the user is actually the person who he or she claims to be. Integrity services assure that an electronic

document has not been tampered in transit or in storage. Confidentiality service assures that the message or document has not been read by any unauthorized person. Non-repudiation assumes that the sender or receiver of a message cannot deny the transaction of an electronic document.

User name and password system for security has several security issues [58]. A password can be compromised, hacked or transferred to another user. Security solutions have been developed for different circumstances. Examples of such solutions are digital identity token, biometric device, public key infrastructure (PKI), digital signature, asymmetric key pair, public key, secret key etc. PKI can meet the requirements of authentication, integrity, confidentiality, and non-repudiation. Setting up of PKI involves legislation and government approval as detailed above.

The e-Governance gateway is another central point that controls the users' access to the e-Governance ICT assets. A gateway performs registration and authentication of users, routes requests for services to appropriate backend installations. It can also provide enrollment of citizens and businesses for a variety of government-to-citizen (G2C) and government-to-business (G2B) services that they need from the government.

Transport environment consists of LANs, WANs, Wireless and RF networks, satellite networks and the Internet. Except the Internet, all other networks can be secured through appropriate means by network administrations. Popular way to tackling the security issues of the Internet are: creation of virtual private networks (VPN) in public domain, installing firewalls at the interface between the Internet and agency networks. Encryption of data communicated over the Internet; IPSec techniques could also provide confidentiality and protection of data passing through the Internet.

Two types of ICT assets are tangible (that is hardware) and intangible (that is software) assets. They are most valuable from the point of view of an organization or a user. Two categories of security treatments, therefore, are physical security for hardware assets and electronic security for software assets. Physical security is required to guard against physical damage or loss of hardware equipment. On the other hand, electronic security controls digital traffic that enters or goes out of an enterprise. Examples of tools involved for electronic security are antivirus systems, intruder detection systems, firewalls, etc.

4.6.2 Security Architecture and Standards

Security architecture is a high level policy document that directs and guides the security of e-Governance. Among others, its main goals are to create confidence and trust among citizens, businesses and government enforcing standards for security in e-Governance. Security architecture also indicates the procedures and processes that need to be followed by all players like government users, citizens, businesses, government partners, operators and service providers participating in e-Governance. Architecture for e-Governance takes care of services for confidentiality, integrity, availability, authentication, and non-repudiation for transfer and storage of electronic information. The achievement of the above objectives involve regulatory, technological and managerial issues arising out of the security needs encompassing user environment, transport environment and ICT assets environment. The security architecture or security framework should be based on statutory regulations, security standards and security policies [39, 61, 70].

Security standards provide specifications for the management of information security. The standard for information security adopted by ISO is known as ISO 27001 [71]. This standard helps to identify, manage and minimize threats to which information is subjected; this is referred to as Information Security Management System (ISMS). The items prescribed by ISO 27001 are: security policy, personnel security, access control, compliance, system development and maintenance at the design and development stage. This standard also covers communication and operations management for transport of information, organization of assets and resources, physical and environmental security, and business continuity management to avoid interruptions to business activities. Business continuity management is defined as a holistic management process that identifies potential impacts that threaten an organization with associated risk, and provides a framework for building resiliency with the capability for an effective response which safeguards the interests of its key stakeholders, reputation, brand and value creating activities. This management structure includes the facilitation of recovery, continuity, and/or restoration in the event of a disaster or crisis through the management of an overall contingency programme and through training, rehearsals, and reviews, to ensure that the plan stays current and up to date.

4.7 Summary

In recent past, considerable progress has been made towards digitization of government processes in the country, but importance of security of information in computer storage or in transit through networks has not received due importance. An important concept for information security in electronic forms for e-Governance is the awareness of the government and people. The users of ICT tools [15] for receiving e-Governance services should be aware of different cyber attacks and threats, and they should set up appropriate countermeasures against such attacks. Similarly, technical personnel of the government, engaged in networking activities and providing e-services, should have in-depth knowledge and understanding of the mechanisms of cyber attacks on ICT assets and their countermeasures. Cyber crimes and threats to electronic information, especially of e-Governance, are based on advanced ICT techniques and law enforcers must be trained and well equipped to tackle them. As a matter of fact, cyber crimes investigation cells should be established with trained personnel in information security.

Information security is very critical to the success of e-Governance. Laws, regulatory framework and polices are already in place in India to combat high-tech cyber crimes for e-Governance projects, organizations and individuals. In this chapter the identification of threats and vulnerabilities have been done in detail for the different models of e-Governance projects. This will enable the appropriate authority to initiate the structured development of Information Security Management System for e-Governance projects. The necessity of ICT cadre service with specialized information security knowledge is becoming more and more relevant with increasing digitization of government processes for providing e-services to citizens and others. It appears that without this cadre service it will be very difficult, if not impossible, to provide effective leadership for information security in e-Governance in future.

In the next chapter the security of online delivery of government services is looked into in detail.

Security of On-line Government Service Delivery

5.1 Introduction

All citizens who live under a governing body, whether national, state, or local, need to interact with government. Some interactions are voluntary (e.g., subscribing to a particular social scheme); while others are mandated (e.g., paying taxes, or getting a driver's license to drive on public roads). Business and other organizations also need to interact with the government on a regular basis. A government's constituency is large and diverse, and includes such special populations as the physically challenged and the illiterate.

Given a large population with widely varying needs, it can be difficult for the government to effectively deliver services to citizens and organizations. The problem can become worse as government and population grows but delivery systems do not change. Service delivery becomes slow and uncertain, and the cost of delivering services can rise. This can lead to corruption (for example, payment of bribes to get a job done). These problems are common, perhaps more so in developing nations like India.

To address these problems, governments are now attempting to streamline service delivery and bring greater speed, certainty, and transparency to the process. Electronic Service Delivery (ESD) is one way governments attempt to deliver services directly to the citizen, without the citizen having to go to a government building. Electronic Service Delivery can look like other shopping or service sites on the Internet.

5.2 Online Government Services

The objective of ESD is to support and simplify governance for all parties - government, citizens and businesses. Information and Communication Technologies (ICT) can help connect all three parties and support processes and activities. Much of ESD is about establishing common standards across government [2], delivering services more effectively, and providing ways for government agencies to work together using the best technologies that are available.

e-Governance refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions.

Traditionally, the interaction between a citizen or business and a government agency took place in a government office. With emerging information and communication technologies it is possible to locate service centres closer to the clients. Such centres may consist of an unattended kiosk in the government agency, a service kiosk located close to the client, or the use of a personal computer in the home or office. The different types of interactions in e-Governance systems have already been discussed in section 1.3.

5.2.1 Levels of Service

Depending on the maturity of a government's electronic service delivery capability, the following levels of service may be provided, in order of increasing sophistication:

Informational

The government IT infrastructure and service delivery capability is fairly rudimentary, and provides only static information via electronic means, in the form of government instructions and such things as application forms, newsletters, etc.

Interactive

With slightly more sophisticated and reliable infrastructure, some interactive service content can be made available electronically. For instance, a website may allow a form to be filled online, printed, and carried to a government office in person.

Transactional

The government information technology infrastructure is mature enough but not widely available throughout the country and the government has reasonably stable and reliable electronic service delivery capability. Online submission of corporate tax returns fall into this category, as most corporate head offices are located in cities where Internet and other IT infrastructure is available. The government departments would have their internal IT divisions to construct and look after their own ESD applications.

Integrated

The government information technology infrastructure is mature, stable and pervasive; the government has been able to develop its electronic service delivery capability sufficiently such that government departments can interact with one another electronically. The electronic service that is delivered to the consumer is not from just one department but is an integrated product from more than one department.

5.3 Integration of Services – Concept of Service Delivery Gateway

Various e-Governance applications may be implemented in order to provide speedy delivery of government services to citizens at affordable costs. It is imperative that the different departments in the Centre, States and Local Government cooperate, collaborate and integrate information across various levels, domains and geographies. e-Governance Service Delivery Gateway enables this by providing seamless interoperability and exchange of data across heterogeneous applications of geographically dispersed departments. This was proposed by the National e-Governance Plan (NeGP) that was approved by the Government in the month of May 2006, with the following vision [57]:

“Make all Government Services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency and reliability of such services at affordable costs to realize the basic needs of the common man.”

Further, with the aim of bringing in transparency and accountability in its functioning, the Government had enacted the Right to Information Act, 2005 which places an obligation on the Central and State Governments and its bodies to provide information to citizens. Under the Section 4(1) of the act, it is stated that

“Every public authority shall – (a) Maintain all its records duly catalogued and indexed in a manner and the form which facilitates the right to information under this Act and ensure that all records that are appropriate to be computerized are, within a reasonable time and subject to availability of resources, computerized and connected through a network all over the country on different systems so that access to such records is facilitated.”

The Information Technology Act, 2000 (as amended in 2008) provides legal recognition for electronic transactions and enables citizens to electronically access information and public

services efficiently and seamlessly. Section 6A of the Information Technology Act 2000 provides for Efficient Delivery of Services to the public through electronics means. This section states that the appropriate government (Central and State Govt.) may authorize any service provider to set up, maintain and upgrade the computerized facility for efficient delivery of services to the public through electronic means. The section also provides that service provider may collect, retain and appropriate such service charges as may be prescribed by appropriate govt.

In this regard Department of Electronics and Information Technology (DeitY) has notified the Information Technology (Electronic Service Delivery) Rules, 2011 on 11.4.2011. The rules specify the system of Electronic Service Delivery, notification of Electronic Service Delivery, creation of repository of electronically signed electronic records by govt. authorities, procedure for making changes in the repository, responsibility of service provider for financial management and accounting and audit of information system and accounts of service provider and their authorized agent. The rules also provide for use of special stationery in Electronic Service Delivery.

5.3.1 National Service Delivery Gateway (NSDG)

The National e-Governance Service Delivery Gateway (NSDG) has been set up under the National e-Governance Plan (NeGP) to act as a core infrastructure for achieving standards-based interoperability (IIP/IIS) between various e-Governance applications implemented at various levels and geographically dispersed locations.

The objectives of the NSDG are

- To evolve Gateway messaging standards and build a government owned Central Gateway based on these standards.
- To act as a catalyst in enabling the building of Standards based e-Governance applications with Gateway as the middleware to ensure interoperability.
- To enable integration across Centre, State or Local Governments thereby enabling Integrated Service Delivery and a Service Oriented Architecture (SOA) leading to joined up government.
- To help protect the legacy investments in software and hardware by easily integrating them with other technology platforms and software implementations.
- De-link the back-end departments/Service Providers (SP) from the front-end Service Access Providers thereby

- Ensuring separation of concerns of service access from the service implementation i.e. separates the Portal, CSC, Kiosks etc from the government services which reside in the backend departments.
 - Encouraging competition at the front-end by allowing independent service access providers to provide services with varying levels of complexity, cost and service quality levels
- Enable adding of shared services on to the core services as and when required, as special common services of the Gateway without affecting the core functionality of the Gateway, thereby providing flexibility and modularity.
 - Encourage back-end services to be plugged into the infrastructure as and when they are ready
- Reduce the cost of e-Governance Projects by rationalizing, distributing and optimizing the services framework
- Use PKI infrastructure for secure transactions. Provision exists for encryption of department payload to ensure confidentiality of department data. The gateway provides digital signature and certificates to all stakeholders interacting with the gateway for identification, authentication and authorization. Transaction and audit logs help track government data.
- Enable transaction logging and time stamping for tracking of transactions and centralized control.
- Help the Departments backend workflow evolve gradually as the Gateway acts as a middleware delinking the backend from the front end.

The services provided by NSDG are for the departments (Service Providers) and for the front end portals (Service Access Providers) and not for direct consumption of the citizens. The following services are delivered:

- Messaging
- Audit Logging
- Gateway Services Directory
- National Services Directory
- Registration
- Reporting

5.3.2 State Service Delivery Gateway (SSDG)

The emergence of many e-Governance applications for different departments to provide online services to citizens, businesses and government would require increasing interactions

amongst departments and with external agencies at various levels in State Government. Departments would need to develop connectors/adaptors for point to point connections among themselves creating a mesh and also tight coupling between applications. This would lead to applications being difficult to maintain and upgrade in case of version change and change in government policies and business rules. The State e-Governance Service Delivery Gateway (SSDG) is an attempt to reduce such point to point connections between departments and provide a standardized interfacing, messaging and routing switch through which various players such as departments, front-end service access providers and back-end service providers can make their applications and data interoperable. The SSDGs are being set up with aims to achieve a high order of interoperability among autonomous and heterogeneous entities of the states based on a framework of e-Governance Standards.

The SSDG project has been formulated under NeGP to fulfill the vision of providing easy and convenient services to the citizens through remote access primarily through Common Service Centres (CSCs) and State Portals. The SSDG

- Acts as a hub for all the interactions between service seekers (the citizen and businesses) and various service providers (Government Departments) and even among Government Departments.
- Handles large number of transactions across the entire network; provides a common set of specifications and a single point access.
- Provides seamless interoperability and exchange of data across the departments.
- Facilitates synchronization and co-ordination of inter departmental working, tracking all transactions of the Government etc.
- Is a messaging middleware between State Portal (acting as service access provider (SAP)) and State Department Services (State Department acting as Service Provider (SP))

The services that will be provided through SSDG are listed in Table 5.1.

Table 5.1: Services to be implemented through SSDG

Name of Department	Services
Labour & Employment	1. Registration of Candidates 2. Renewal of Registration 3. Application for admissions to ITIs

Name of Department	Services
Revenue Department	4. Issuance of Index 2 5. Non - Encumbrance Certificate 6. Registration of Marriage under Special Act 7. Issuance of Solvency Certificate 8. Record of Rights (ROR) 9. License for booking of Public entertainment Program/Public performance 10. Relief under Solacium fund 11. Permission for land to be used for Non Agriculture purpose 12. Permission for Block Division Land 13. Application for Renewal of Stamp Vendor License
Social Justice & Empowerment	14. Issue of ID card to the Disabled / Various Financial Schemes 15. Pension Scheme to Old (Vriddha Sahaya Yojana) 16. Caste Certificate (SC) 17. Caste Certificate (OBC) 18. Loan Application for Foreign Study 19. Loan Application for Commercial Pilot 20. Kunvarbai Nu Mameru 21. Inter caste Marriage 22. Air-Hostess Training – Application form 23. Stipends for Advocates 24. Sadhan Sahaya Yojana (Manav Garima Yojana) 25. Sant Surdas Yojana 26. Ambedkar Awas Yojana 27. Pandit Din Dayal Awas Yojana
Finance Department	28. Insurance Scheme
District Passport Application Collection Centre	29. Passport Application Collection
City Survey Information System (Property Card Computerization)	30. Online Mutation request
ITI Admission	31. Online Form Filling
Employment Exchange	32. Registration 33. Renewal 34. Vacancy submission
Panchayat Department	35. Sardar Awas Yojana 36. Indira Awas Yojana 37. Inclusion of name in Voters' List 38. Application for welfare schemes under NREGA 39. Application for Income Certificate 40. Application for Birth Certificate 41. Application of Death Certificate 42. Application for Marriage Certificate 43. Application for Pahani Patra 44. House Tax Collection 45. Water Tax Collection 46. Application for New Water Connection
Ration Card & PDS	47. New Ration Card 48. Addition/Deletion in Members 49. PDS Coupon
Women & Child Welfare Department	50. Widow Pension Scheme 51. Services to Pregnant mother and child

Name of Department	Services
Education Department	52. Application for various Scholarship Schemes 53. Application for admission to CPed. / DPed 54. Application for PTC 55. Application for Duplicate Mark sheet / certificate 56. Application for Migration Certificate
Health – Food & Drugs Control Administration	57. Drugs(Allopathic) Mfg. License & Related Certificated
Home Department	58. Application for New Arms License 59. Renewal of Arms License 60. Certificate for residential Proof 61. Domicile Certificate
Common to ALL Departments	62. RTI 63. Grievance Service
Land Records	64. RoR issue 65. Mutation 66. Notice Generation
Property Registration (GARVI)	67. Document Registration with application registration fess 68. Land Ownership verification for Agriculture 69. Capture Photo and Thumb Impression of Parties, 70. Scanning the registered Document. 71. Certified copy of registered document
ATVT	72. Income certificate, non-creamy layer certificate, caste certificate, senior citizen centre certificate, widow pension certificate, all kinds of affidavits etc.
Pension Information System For Dept. of Posts	73. Pension Authorization 74. Pension Case status 75. Voucher Audit
Online Job Application System (OJAS) (NOT MMP)	76. Online application 77. Call letter printing
DLIMS – Drug Logistics & Inventory Mgmt. System	78. Rate Contracts, Ordering, Stocking Procurement, Distribution, Billings, Payments, etc.
XLN-Xtended Licensing Nodes for Food & Drugs dept. (GJ & MH)	79. Licensing & Laboratory related activities
District Court Case Status and Cause List	80. (I) Cause lists of District and Taluka Courts 81. (ii) Orders and Judgments of District and Taluka Courts
CPMS for Tribal Development Dept. Projects	82. Computerized Project Monitoring 83. Agency's Data Entry Process 84. Data Sharing
Revenue Cases Management System	85. Copy of Order/ 86. Judgment
Vikaspah-Online Approval, Reporting & Monitoring of Panchayat Schemes	87. Online Proposal, Sanction, Grant allocation and booking of expenditure

Name of Department	Services
Court Case Information system – Gujarat High Court	88. Case status 89. List of Business 90. Daily notices 91. Advocate sick/leave not 92. Orders/Judgments
Online Recruitment process for Judicial officers)	93. Online application 94. Call letter printing

5.3.3 Interactions between NSDG and SSDG

NSDG provides a standardized interfacing, messaging and routing switch through which various players such as departments, front-end service access providers and back-end service providers can make their applications and data inter-operable. This results in a high order of interoperability amongst autonomous and heterogeneous entities of the Government (in the Centre, States or Local bodies) based on a framework of e-Governance Standards. NSDG thus helps the departments to provide integrated services and joined up services to the citizens via a single window.

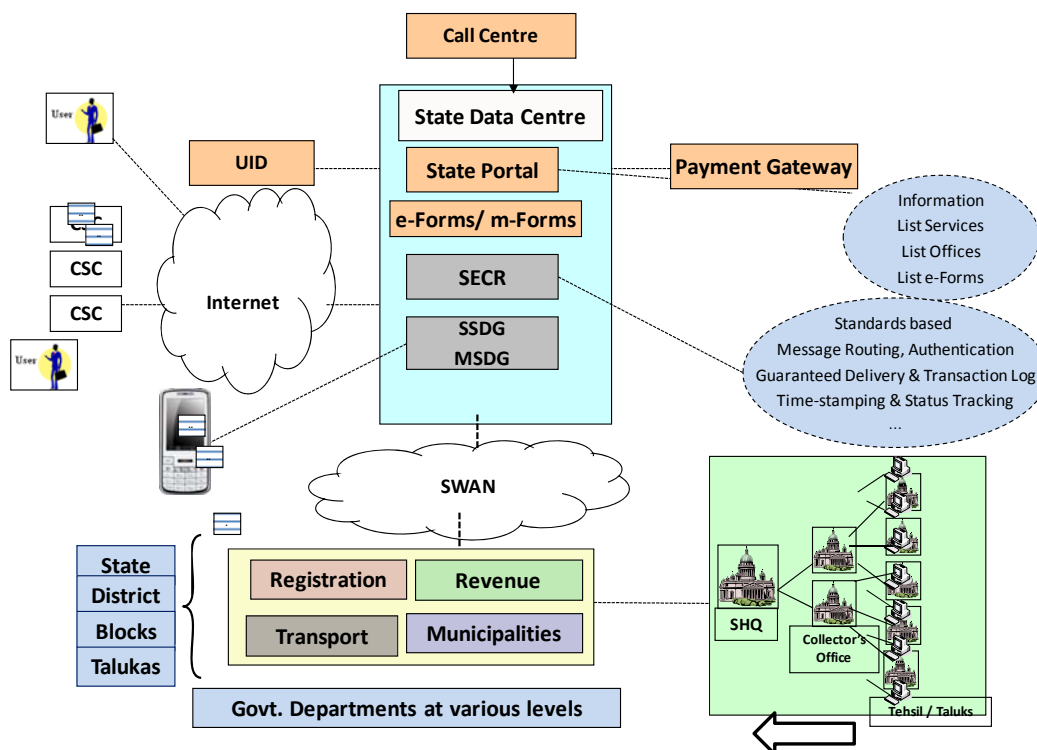


Figure 5.1: e-Governance Service Delivery framework

SSDGs are being installed in all the states. These gateways are connected to NSDG Gateway constellation via a National Services Directory (NSD) which in turn can be leveraged to connect departments across the country. This is detailed in Figure 5.1 (SECR stands for State

Electronic Certificate Repository). The future e-Governance space of India would see many Government Departments/local bodies and Businesses offering many services, which will be used by the Citizens, Businesses and other Government Departments/local bodies. This would give rise to multiple Service Access Providers (SAP) and Service Providers (SP) and these necessarily may not reside with one Gateway but may be distributed among more than one Gateway (Gateway Constellation) under different administrative domains across the Centre, State, and local governments including gateways in specialized verticals.

The choice of a Gateway will be dictated based on the need for connecting multiple e-Governance services on multiple technologies/platforms to increase interoperability factor. In the absence of a gateway in any vertical or State level the service can still be offered through the default National Gateway.

Table 5.2: Services to be implemented through NSDG

Central Gateway (NSDG)	State Government/ Local Government Gateways (SSDGs)	Department/ Ministry/ Domain specific Gateways
G2G in the Centre	G2G within the State	G2G within the Centre spread across the country, with each unit of the Department having its own IT infrastructure
G2C in the Centre	G2C within the State	G2B on matters relating to the Centre in business matters
G2B relating to departments in the Centre	G2B relating to the departments in the State, Local Bodies and Utilities	G2C on matters relating to citizens

When multiple Gateways become operational, NSDG will be equipped to route the messages to appropriate Gateways and reach out to the service offerings of local bodies, state governments and central governments, all working together in a peer-to-peer network. However, it is imperative that all these unifying Infrastructures, under various administrative domains [32, 36] work in close co-operation and in unison to support the outcome based paradigm of service delivery to the Citizens, Businesses or other Government Department/local bodies. There could be **three distinct types of gateways**: The Central Gateway, the State Gateways and Department-specific (Domain) or Purpose-specific Gateways. The service scenarios cover three distinct groups: (a) Citizens (b) Businesses and (c) the Government departments / Ministries / Agencies. Table 5.2 summarizes the usefulness of the Gateway within each of these entities.

Figure 5.2 depicts the conceptual gateway cluster with various services hosted by various gateways, and these services listed on the National Service Directory (NSD) also a part of the gateway constellation for gateway address resolution.

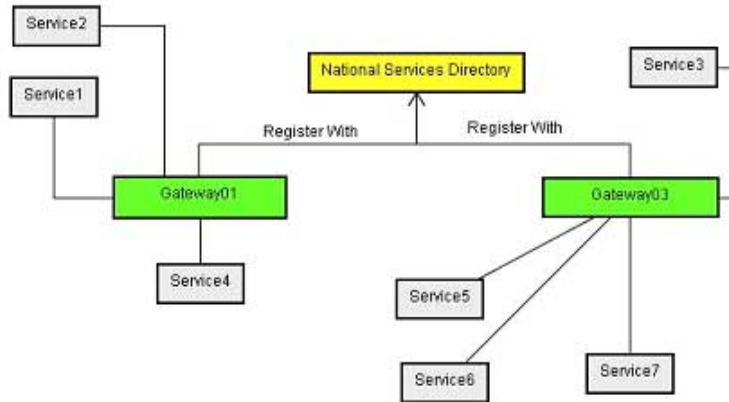


Figure 5.2: Conceptual Gateway Cluster

5.4 Architecture and Implementation of SSDG and NSDG

The overall functional architecture for NSDG and SSDG is shown in Figure 5.3. The Gateway links four major entities:

Service Providers (SP)

The back-end government departments or any other third-party agencies offering e-services to citizens and businesses, and to other government departments, are collectively referred to as Service Providers (SP). Third-party SPs may offer specialized services such as authentication, payment gateway services, or joined-up services. The Gateway would provide major benefits to the departments such as:

- o **Multiple Delivery Channels:** The position of the Gateway as the middleware will facilitate easy provisioning of government services through various delivery channels [13] seamlessly.
- o **Better Audit Management & Time Stamping:** Results in better tracking (auditing) and security of each transaction.
- o **Web enabling of Legacy Applications:** With the use of Gateway Server, even legacy applications can be Internet-enabled as Gateway server can act as a Web layer around them, so Government Departments need to put least effort for web enablement of their legacy applications.
- o **Interoperability:** The gateway positioning as the middleware will facilitate easy inter-departmental data exchange.
- o **Departmental Workflow:** The Gateway will also help the Departments' backend workflow evolve gradually as the Gateway acts as a middleware de-linking the backends from the front end. This means that even the Departments, which do not

have complete automation or workflow at the backend, can still deliver e-Service to the citizens in a limited manner. To cite an example, a server may be put up at the department for message exchange with the Gateway in the absence of readily available infrastructure at the department.

- o **Seamless availability of information:** The placement of constellation of Gateway Servers at State Level will facilitate in getting information and doing transactions by citizens of one State with Government Department of other States seamlessly.
- o **Centralized Management:** The positioning of Gateway Server and building portal of all the departments at Central location, i.e., in State Data Centre, will help in better centralized Administration, Monitoring, over all maintenance work and deployment of hardware of Web Site at optimal level.
- o **Shared Services:** In the future, the Gateway has the capability to add additional functionality to support shared common services like authentication, payment gateway interface, etc.

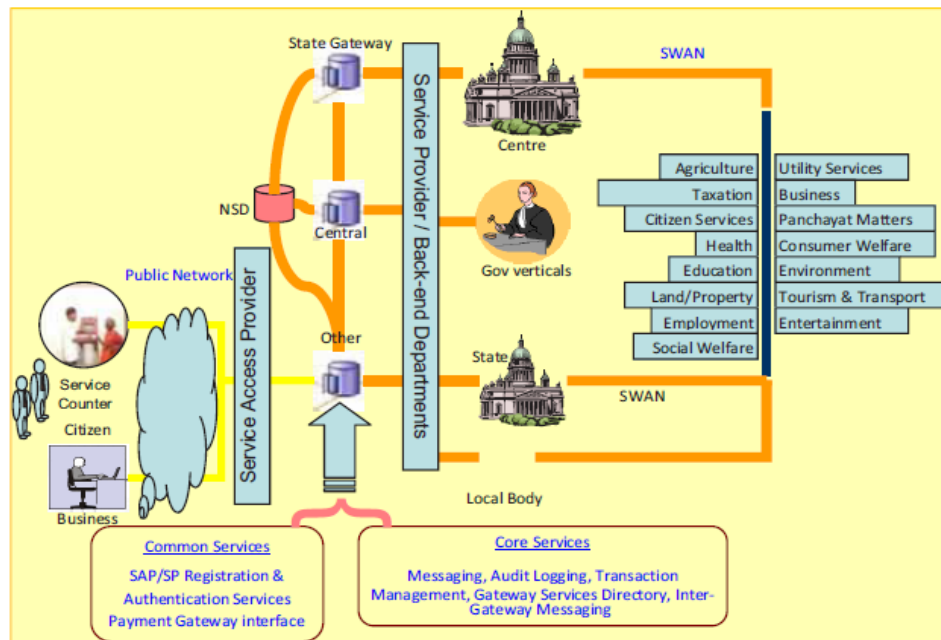


Figure 5.3: Gateway infrastructure operating at the Centre and States in e-Governance service delivery

Service Access Providers (SAP)

A Service Access Provider is an entity, which facilitates government service access by Service Seekers [38], by providing a front-end infrastructure. Linked to the Service Access Providers will be the Delivery Channels [82], which would be the access mechanism for the

citizens and businesses to avail the e-Governance services. The Gateway would provide the following major benefits to SAPs:

- o **Easy interface** with departmental data and Business logic: With the middleware like NSDG in position, the departmental data and business logic reside at the backend and a SAP is in a position to easily integrate with the departmental data and provide value added services.
- o **Integrated and joined up services:** With NSDG in position, a SAP could easily provide integrated services to the citizens by fetching data simultaneously from multiple departments, or send the service request to one department which could in turn fetch data from other departments and send the same to SAP.
- o With NSDG as the middleware it gives SAP flexibility in modifying the front-end application without touching the backend applications.

Gateways (NSDG, SSDG, Domain Gateways)

The future e-Governance space of India would see many government departments, SPs, and SAPs offering e-services to citizens and businesses. These necessarily may not be directly connected with one Gateway but may be distributed among more than one Gateway across the Centre and State including Gateways in the departmental applications like MCA21, Passport called Domain Gateways.

National Services Directory (NSD)

The primary function of the National Services Directory (NSD) is to provide a registry, which acts as a service resolution point for all the services in the Gateway constellation. NSD has information about services hosted in all the Gateways of the constellation (i.e. NSDG and all SSDGs). All the gateways that need to resolve services, which are not registered with them, need to resolve it at the NSD. The Gateways need to register with the NSD before they can attempt to resolve a service from the directory. This is depicted in Figure 5.4.

The services offered by the backend government departments (Service Providers) will need to be uniquely identified and registered under the administrative domain of the concerned Gateway. During a service life cycle, services may be closed or new services may be added. The Gateway in reality becomes an aggregator of service information within its jurisdiction.

The NSD is proposed to be set up as part of the NSDG initially, which may be moved out as a separate entity by the Government if need be.

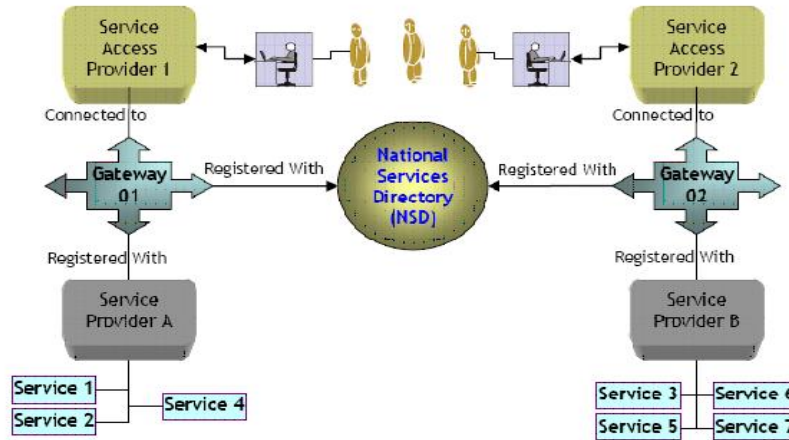


Figure 5.4: Positioning NSDG in various e-Governance Projects

5.4.1 Interoperability Standards for implementation of Gateway

Several interoperability standards have been developed as part of the Gateway project [48, 49]. The Gateway Service Provider (GSP) is required to understand these standards in their entirety and implement the NSDG solution in compliance with them.

1. Interoperability Interface Protocol (IIP)

e-Governance infrastructure is necessarily a distributed one and there are a multitude of participants to this infrastructure. The communication between some of the key participants is critical to hold this infrastructure together need to be specified and standardized. The objective of Interoperability Interface Protocol (IIP) and Interoperability Interface Specification (IIS) is to standardize on the protocol and to specify the interface nature for this communication to take place.

IIP is the communication protocol that the Service Access Providers, e-Governance Gateway and the Service Providers need to comply with. This protocol is divided into two parts, one part targeted towards the Service Access Providers and one for the Service Providers. e-Governance Gateway as the infrastructure needs to support both the interfaces.

IIP is an asynchronous request-poll-retrieval protocol, with provisions for synchronous communication, which supports requests to be sent and receive a response through a polling mechanism or synchronously. The foundation of the protocol is based on message types and context based processing of messages. There are mechanisms for sending a request, communicating acknowledgements, querying the state of a request, sending and

communicating responses and to handle error situations. The message types supported by this protocol are listed below:

- o Submit Request- Used to send an service request
- o Submit Acknowledgement - Used to acknowledge submission requests
- o Submit Poll - Used for polling for responses
- o Submit Response - Used to package the service response
- o List Request - Used for querying submission state
- o Delete Request - Used for ending a submission session
- o Delete Response - Used as an indicator for submission session ending
- o Submit Error - Used for responding to errors

Exchange of IIP compliant messages is intended to be the primary mode of communication between the Service Access Providers and the e-Governance Gateway as well as between the Service Providers and e-Governance Gateway. It is to be noted above that not all messages are required to be supported by the Service Access Providers and the Service Providers. Some of the above messages are mandated to be supported by the Service Access Providers and some for the Service Providers.

IIP provides the interoperable interface for communication and all the IIP messages are XML based, therefore readily usable by any application. This interface is the key for success of e-Governance Gateway.

2. Interoperability Interface Specifications (IIS)

IIP provides the protocol, the message formats and the associated semantics of the messages. However, it does not address the issues of the precise exchange of this information through a technology interface. Interoperable Interface Specification (IIS) address this issue. IIS provides the technological specification for exchanging of the IIP compliant message. To this end IIS provides the following :

- o Mapping of the IIP message to a carrier protocol, SOAP
- o Provides guidelines for messaging, in terms of message size, etc.
- o Provides facilities for optimization, through batching mechanism etc.

IIS compliments IIP by translating the message exchange into a viable form of messaging mechanism, such that optimization can be achieved by the implementing application. In terms of carrier protocol, IIS follows SOAP, as standardized by W3C, such that wide industry support is available in forms of ready libraries and implementations. IIS is always used in

conjunction with IIP; therefore it is uniformly applicable to the Service Access Providers, Service Providers and e-Governance Gateway.

3. Inter-Gateway Interconnect Specifications (IGIS)

The e-Governance Gateway infrastructure under various administrations in India will form a hierarchical constellation of which every state and centre Gateway will be a part. However, for this constellation to be realized and successfully operational there needs to be a set of predefined guidelines and standards, which will govern various aspects of the constellation, such as its structure, behavior and policy. The IOI Gateway Interconnect Specification (IGIS) is targeted towards providing such a comprehensive documentation of all aspects of the Gateway Constellation. The primary aim of this standard is to provide the specifications and protocols required for construction of the Gateway Constellation. In this endeavor, the document provides specifications at the following levels:

- o Gateway Constellation Structure
- o Service Resolution and Service Information Propagation
- o Operational Guidelines for Gateway Constellation
- o Gateway Interconnect Protocol (GIP)

This specification defines the structure of the Gateway Constellation, the communication mechanisms between various gateways in the constellation, facilities to propagate a service request to its required destination and the policy guidelines applicable to each of the participating gateways in the constellation and the constellation as a whole. This specification is intended to provide the basis on which the Gateway Constellation will be realized. The specification and its associated protocol (s) may be realized with the help any suitable technology and means. In effect, this specification is a technology neutral specification, guideline and protocol enumeration for the Gateway Constellation.

Conformance to IGIS is required by any Gateway that needs to be a part of the Gateway Constellation and is therefore mandated for all state level and centre level Gateways.

4. Gateway Common Services Specification (GCSS)

These specifications are a compilation of a common set of services for NSDG Gateway. These services are considered generic enough in nature, such that they required by more than one government department and Service Access Providers. The generic nature of the services warrant their existence at NSDG Gateway Level, such that substantial reuse of these services can be achieved and individual applications in the e-Governance space of India (present and future) can are spared, metaphorically, the reinvention of the wheel. The set of service

specifications contained in this document is expected to expand over time as and when new generic services are integrated into the e-Governance framework of India, therefore, this document intends to serve as the single and authentic source for all such service specifications and undoubtedly a living document, which shall witness many updates and augmentations.

5.5 Requirements to Ensure Secure Service Delivery

Since online service delivery involves transfer of personal and financial data of citizens, it is necessary to ensure security of such transactions. The process for deriving security requirements for public service systems emphasizes securing the transaction (as being directly experienced by and relevant to the parties) rather than the data (as the internal representation of the transaction). The aim is to derive a set of security requirements for the systems and services that fairly meets the expectations of the transacting parties.

These security requirements can be derived by performing a detailed risk assessment of the online services. Information security risks are characterized by:

- The information asset under threat and its significance to stakeholders;
- The potential threat sources and actors including assessment of motivation and capability;
- The opportunity that will be exploited (where opportunity may be an unintentional vulnerability or a necessary property of the system);
- The damage that may be experienced consequent on the risk materializing;
- The assessed likelihood of the risk being realized;
- Opportunities for recovery and compensation should the issue arise.

Stakeholders, in particular the target users, vary greatly in their capability to interact correctly with the system and their commitment to the aims of the offered service. Some assessment of the competence and motivations of the stakeholders and other actors is a necessary input to the risk assessment. The following categorizations can be used as a starting point for the analysis.

- a. Committed – The subject understands the aims and purpose of service, understands the rationale for measures and is trained to use the systems, aware of the pitfalls, and committed to making it work.
- b. Conscientious – The subject is motivated to make the service work, generally supportive but is untrained and unaware of dangers.

- c. Indifferent – The subject is not interested in aims, objectives, and outcomes of service, not interested in becoming an informed or competent user, and may resent being required to use service.
- d. Hostile – The subject may be actively committed to undermining the aims of the system motivated by ideology, financial gain, or personal circumstances.

Security requirements are derived from the reasonable expectations of all significant stakeholders in respect of transaction security. The notion of transaction security is broader than (though closely related to) protective security of data held and processed by the systems. Analysis of security requirements for online systems should start with determining and agreeing to the reasonable expectations of the interested parties in respect of security of their transactions.

Tables 5.3, 5.4, and 5.5 are a framework for setting out the expectations and provide pointers to the related threats and security requirements. These tables are designed to help demonstrate that the reasonable expectations of all those involved in a public service delivery are adequately addressed. It is essential that the citizen and business expectations as well as government requirements are addressed. The expectations are described by the following columns:

- a. Expectation – Describes an expectation for security related behaviors viewed from that perspective. There is an assumption of reasonableness, but not that the viewpoint is of someone who understands information security. This policy is predicated on the assumption that these are reasonable expectations, and the systems must meet them or explain the shortfalls and how they might be addressed elsewhere. For example, it is a reasonable expectation that the systems will safeguard user information but it may not be a reasonable expectation that there will never be any system compromises. However, it is a reasonable expectation that, in the event of compromise, recovery action is possible, and that users will be recompensed for any harm experienced.
- b. Concern – is the underlying belief, worry or unease that informs the expectation. Concerns may be valid, unjustified, or overstated, but they remain concerns that must be addressed. Concerns may be based on perceptions of risk and possible harm or they may reflect wider concerns about privacy and other softer issues.
- c. Risks – identifies relevant information risks that will need to be managed.

Users' Perspective

The user (general public, individual user, or business user) viewpoint mainly expresses concerns that their interests and information will not be safeguarded, failures and

shortcomings will not be underwritten and, in the event of dispute or malfunction, there will be a presumption of guilt and inadequate or unfair redress processes. Table 5.3 details the risks from the viewpoint of a user.

Table 5.3: Risks: User Perspective

Expectation	Concern	Risks
Privacy – Online public services will not unnecessarily compromise the privacy of actual or potential users, or the general public, in respect of their personal, financial, or business information.	Government will collect information for which it has no business need, and no rights of access. Government will accumulate information that leaves the user open to identity theft, fraud, invasion of privacy, or other personal distress. Personal information will be shared without explicit permission and will be collated with other sources of information in order to draw inferences about the subject that may be counter to their interests. Government will not look after personal information responsibly or will use it for purposes that were not agreed to.	Deliberate or accidental breaches of confidentiality by third parties will compromise the customer's privacy. Function creep and gradual accumulation of stored personal information presents new (and unmediated) opportunities for invasion of privacy. Analysis of large collected datasets may expose inferences about subjects that violate their reasonable expectations of privacy. Electronically delivered services will not be taken up by the public owing to their concerns about privacy.
Authenticity – Users can be assured that they are interacting with a genuine public service.	Users can be deceived by a plausible false presentation of an online public service and thereby reveal Personal Private Information (PPI) to a potential fraudster ('Phishing').	Personal and private information will be lost to a fraudulent operator with possible personal and financial consequences. The integrity and reputation of public sector services will be undermined.
Confidentiality – sensitive information will only be accessible to those with a legitimate need, and used for a legitimate purpose.	Sensitive information held by the government may be compromised through exposure (deliberate or otherwise) to those who have no need to see it, or may be intent on causing harm. Online public services present opportunities for 'ID Theft'.	Adversaries may exploit vulnerabilities to gain access to information without authority. Information may be accidentally or deliberately exposed to potential adversaries.
Integrity – stored personal information will not be corrupted or changed incorrectly. It will be protected in a manner that reflects its intrinsic value to the individual.	Information held by the public sector could become corrupted or destroyed with undesirable or serious consequences. Information held by the public sector could become out of date or be inaccurate.	Adversaries may deliberately alter sensitive personal information and thereby disadvantage or damage the information subject. Information may be accidentally corrupted leading to damage or disadvantage to the information subject. Users may be unjustifiably accused of damaging or fraudulent activities. Circumstances of a user may change leading to information held becoming inaccurate.

Expectation	Concern	Risks
Availability – critical services will always be available when they are needed.	Urgent service needs will not be met. Alternate service delivery opportunities will be withdrawn in favor of e-delivery without adequate accessibility, reliability and coverage. Time critical response demands, which may incur a penalty, cannot be supported by the e-systems	Users may be disadvantaged or damaged as a consequence of inability to access public sector services when needed owing to intentional acts by adversaries or accidental misuse of security functions by users.
Transparency – personal information is held by/supplied to the public sector for its agreed purpose only.	Once the public sector has possession of information, it will use it for purposes that were not declared when the information was supplied or as agreed subsequently.	Users will be harmed or perceive privacy violations through use of their information for a purpose they were not aware of, had not agreed to, or did not understand.
Identity – systems will confirm the identity of those with access to information before enacting a transaction. The strength of the identity measures will be appropriate to the value of the information, and the need for confirming true identity (as opposed to authority) when completing the transaction. Identity compromise by the public service will be admitted and repair properly supported.	Systems will have weak controls which will lay individuals open to identity fraud and malpractice. Identity controls will be applied insensitively; full identity will always have to be proved where it is not strictly necessary. Interactions will be unnecessarily intrusive leading to privacy concerns. Public authorities will offer poor support for identity repair following compromise and leave responsibility with the customer.	Adversaries will be able to impersonate legitimate users and cause damage through abusing their access rights. User privacy will be compromised through demanding full identity when not necessary for the business in hand. Users will continue to suffer the consequences of identity compromise and will not be supported in identity repair or compensated.
Reliance – it is safe to act upon the displayed service outcomes.	The online public sector services may not display the true situation, e.g. monies showing as transferred may not be accessible, or information may be misleading leading to later penalty.	Users will be harmed as a consequence of taking action on incorrect or inconsistent system information or instructions.
Payment Safety – monetary transfers are correctly carried out between the correct parties and do not lay individual financial details open to exploitation.	Bank account details will be misused or not properly controlled leading to financial exposure. Erroneous transactions cannot be challenged or reversed.	Adversaries can exploit vulnerabilities in the systems to commit fraud. Fear over financial exposure and fraud will deter users from using the systems.

Expectation	Concern	Risks
Accountability and Fairness – False accusations of fraud or unwarranted impositions of penalties will not be made and cannot be upheld. Any dispute will be easily and fairly resolved.	The liability model will not be fair to the individual, there will be a presumption of guilt in the event of a dispute and no evidence against which a case can be made and redress sought.	Fear over lack of transparency and fairness will deter users from using the systems. Users are unable to query transactions and resolve inconsistencies to their and the system owners' satisfaction.
Inclusivity – The advent of electronic access to public sector services will not disadvantage those with particular personal circumstances or disabilities [41, 47].	Public sector service access will be more difficult and discriminatory and alternate access routes will be withdrawn.	Users may be denied service through inability or incapability to access the electronic systems. Adversaries may harm users through exploitation of weaknesses in the fall back arrangements for the electronic systems.
None Discoverability – search or query access to systems and data will not be accessible to Unauthorized individual or used for unauthorized purposes.	Unauthorized parties or subverted authorized parties will gain search or unconstrained query access to large or complete datasets and thereby be able to discover or draw inferences about vulnerable subjects.	Query access to large datasets will be misused in order to locate individuals, or identify at risk individuals (e.g. witness protection) at an impact level in excess of the individual records.

Service Owners' Perspective

The service owner viewpoint reflects the concerns of those charged with delivering business improvements and efficiencies through increased use of ICT, and reflects major concerns that the security measures will be intrusive or unaffordable, and that security failures in large business systems will lead to departmental sanction and failure. Table 5.4 details the risks from the viewpoint of a service owner.

Table 5.4: Risks: Service Owner Perspective

Expectation	Concern	Risks
Compliance – systems are able to comply with an acceptable interpretation of relevant legislation and policies in regard of protecting official and personal information and managing information risk.	Compliance responsibilities are unclear and not closely related to the practical value and impact of security controls. Meeting the compliance requirements is infeasible or expensive and time consuming, and inhibits business delivery. Individuals may be held accountable for circumstances outside their control.	Information management controls will be held to be deficient through lack of clarity on roles, requirements, and responsibilities. Lack of clarity of roles and accountabilities will lead to an overly cautious interpretation of compliance requirements resulting in higher costs and/or unnecessary service limitations.
Available Measures – Suitable security measures are available on the market and widely accepted as reasonable, proportionate, and meeting the national and citizen interests.	The available policies, products, and knowledge, do not allow solutions to be built. Impractical and inappropriate solutions will be adopted to achieve administrative compliance.	Information risks will be improperly managed through inability to source the necessary measures. Legalistic focus on compliance will result in the acquisition of inappropriate or ineffective measures.

Expectation	Concern	Risks
Affordability – Security processes and measures will not place an unsustainable cost [54] burden on departments.	Affordable products and services do not exist, and development costs of new capability are high. Assurance requirements push costs up. A sustainable COTS market will not exist.	Information risks will be improperly managed through inability to afford the necessary measures or the acquisition of inappropriate measures.
Business Impact – Security measures do not impact the business to the extent that the desired business outcome is unachievable or unaffordable.	Policies and compliance regimes lead to unacceptable business impact. Regulatory and policy restrictions preclude the use of apparently suitable solutions.	Responding to IA regimes and processes will impact on the viability of the service offering. Proposed service is beyond the acceptable bounds of information risk.
Risk Awareness – Information risk awareness will be high and it will be possible to understand the efficacy of the risk mitigation measures and their value to the business.	There is a lot of material about managing information risk which concentrates on deriving the measures and testing their quality, but little on determining actual business harm and to what extent the measures affect it.	Un-testable risk assumptions will result in the deployment of uneconomic or restrictive measures.
Assurance – the value, utility, and quality of the installed security measures can be confirmed as suitable and VFM is clear.	It is hard for public sector security authorities to get a meaningful independent confirmation of the quality, effectiveness, and appropriateness of selected measures.	Poor appreciation of security will lead to inappropriate application of assurance schemes and processes and limit the opportunities for success.
Supply – Business services will most likely be delivered through third parties who can, and are able to, accept their part of the responsibility for information risk.	Security capability, processes and practices do not align with contracting practice for service provision. Service providers cannot accept risk transfer, or will price unrealistically.	Commercial and contractual drivers will dominate and information risks will not be properly managed.

Service Suppliers' Perspective

The Supplier viewpoint represents the interest and concerns of product and service suppliers who are contracted to deliver or otherwise involved in the delivery of electronic public services. Table 5.5 details the risks from the viewpoint of a service supplier.

Table 5.5: Risks: Service Supplier Perspective

Expectation	Concern	Risks
Clarity – requirements and responsibilities for security of supplied systems and services are clear enough, and stable, to allow the commercial risk to be scoped and implemented.	Government IA policy, practices, processes and capabilities are inadequately described, opaque, and subject to change. Commercial risks in responding are unacceptably high leading to uncompetitive pricing or financial and business risk.	Misaligned expectations of service owners and suppliers with regard to security will lead to contractual difficulties.

Expectation	Concern	Risks
Achievability – affordable equipment and assurance services will be available to meet contractual requirements.	It will not be possible to respond sensibly to procurements because the needs are unclear or excessive and the necessary products and services are unavailable.	Supply opportunities will be lost owing to inability to supply against (possibly unrealistic) requirements.
Positive Risk Culture – prevailing culture will be one of partnership in dealing with information risk, and not simply risk and cost transfer. Commercial risk associated with partnering with customer on information risk can be priced.	The department will seek to pass information risk to the supplier when it is not appropriate so to do.	Information risk management will suffer from lack of ownership.

5.6 Security Controls for Delivery Gateways

The risks identified in the previous section need to be mitigated in order to provide secure delivery of online e-Government services. This can be achieved by implementing relevant security controls, which either plug vulnerabilities, or mitigate threats, thus reducing risks to information systems [12, 39]. The selection and employment of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Table 5.6: Security Control Classes and Families

Class	Family
Application	Application Identification and Authentication
Application	Application Access Control
Application	Data Handling & Protection
Infrastructure	Identification & authentication
Infrastructure	Access Control
Infrastructure	Audit & Logging
Infrastructure	System & Communications Protection
Infrastructure	System & Information Integrity Protection
Operations & Management	Security Policy & Procedure
Operations & Management	Security Organization
Operations & Management	Personnel Security
Operations & Management	Physical & Environmental security
Operations & Management	Media Security
Operations & Management	Configuration Management
Operations & Management	Incident Management
Operations & Management	System & Service Acquisition
Operations & Management	Business Continuity Management
Operations & Management	Compliance

Controls for delivery gateways are detailed in “GD 200: Catalog of Security Controls” [16]. These controls have a well-defined organization and structure. They are organized into classes and families for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., **Application**, **Infrastructure**, and **Operations & Management**) and eighteen security control families. Each family contains security controls related to the security functionality of the family. Table 5.6 summarizes the classes and families of security controls in GD 200.

The security control structure consists of three key components: (i) a Control section; (ii) an Explanation section; and (iii) a Control Improvements section. The following example from the Application Access Control family of application class illustrates the structure of a typical security control.

A.AC-6: AUTOMATIC SESSION TERMINATION

Control: The application automatically terminates a remote session after [defined time period] of inactivity.

Explanation: A remote session is initiated whenever an application is accessed by a user (or an information system) communicating through an external, non-organization-controlled or un-trusted network (e.g., the Internet).

Control Improvements:

Automatic session termination applies to both local and remote sessions.

It is important to select and implement appropriate controls so that online services can be securely delivered.

5.7 Assuring Secure Service Delivery

Assurance is the basis for confidence that the security measures work as intended to protect the online service delivery system and the information it processes. All security parameters (integrity, availability, confidentiality, etc.) have been adequately met by a specific implementation when:

- required functionality is present and correctly implemented,
- there is sufficient protection against unintentional errors (by users or software), and
- there is sufficient resistance to intentional penetration or by-pass.

Information security is a balancing act that requires the deployment of “proportionate defense” in order to achieve adequate assurance. The defenses that are deployed or

implemented should be proportionate to the threat. Security of online services is a techno-managerial issue where, a fine balance is to be drawn between system efficiency, security expenses and information protection.

Assurance components cover the activities required to confirm the secure end-to-end delivery of a service [52, 53]. It covers the review of the design, implementation, configuration, operation and disposal activities to ensure that the security requirements are met. Two aspects are considered:

- a. **Organizational Assurance** – This covers the review of the organizations involved in the delivery of a service to ensure that the required management, procedural personnel and physical security arrangements are in place to secure the service.
- b. **Technical Assurance** – This covers the technical review of the totality of an e-Governance service to ensure that it is designed, implemented, configured, maintained and operated in accordance with the security requirements.

These reviews should be carried out by independent personnel to provide assurance of secure service delivery [56, 66, 68].

5.8 Summary

Achieving integration of electronic service delivery capability is not enough for a government. It also needs to ensure that these electronic services are securely delivered and address the concerns of all the stakeholders. Security is the most important challenge that faces the implementation of e-services because, without a guarantee of privacy and security, citizens will not be willing to take up e-Governance services. These security concerns, such as hacker attacks and the theft of credit card information, make governments hesitant to provide public online services. According to the US General Accounting Office (GAO) report of 2002 “security concerns present one of the toughest challenges to extending the reach of e-Governance. The rash of hacker attacks, Web page defacing, and credit card information being posted on electronic bulletin boards can make many federal agency officials—as well as the general public—reluctant to conduct sensitive government transactions involving personal or financial data over the Internet.”

Focusing on technology without realizing the importance of its security has led to the failure of many e-Governance projects across the world. In this chapter, we have identified the security expectations, concerns and risks of online delivery of government services from

stakeholders' perspectives, and implementing appropriate controls to mitigate such risks as per the international standards.

In the next chapter, a policy perspective is discussed with respect to the Unique ID project in the context of e-Governance.

Unique ID and Online Service Delivery – A Policy Perspective

6.1 Introduction

The goal of e-Governance is to enable citizens and private/public sectors to access government services in effective and efficient manner on an anywhere anytime basis. This requires integrated services delivery to the customers in a form convenient to the service recipients through the use of internet and other channels like mobile phones, etc. It should also enable citizens to participate in the government's policy framing and decision making.

The main objective of e-Governance is to allow the public sector to provide citizens with information based on their need, hence increasing their effectiveness, efficiency, and quality of service. However, it is also important that security properties of such information (including private data of clients) be protected from unauthorized disclosure and modification. This chapter deals with the authentication and authorization aspects of online services delivery.

6.2 Requirements of Identification and Authentication of General Citizen

As has been stated in section 1.3, the various kinds of e-Governance services are G2G, G2B, G2C and G2E. While, G2G, G2B and G2E services usually follow standard security procedures for access and usage, the security aspects of G2C services need to be looked into in detail. It needs to be ensured that such services reach the right people and their personal data are protected. In other words, there should be appropriate mechanisms for Identification and Authentication (I&A) of general citizens before they are allowed access to e-services.

By and large, the marginalized or vulnerable groups subsist on the margins of society and are often deprived of access to basic necessities such as, health, education, housing, food, security, etc. owing to their inability to prove identity. For the poor, whether in rural or urban areas, lack of any documents to prove their identity works in a circular way where they find it difficult to extricate from the throes of poverty and condemns them to remain in a vicious circle of poverty. An inability to prove identity can be a big barrier to accessing public

benefits and subsidies. The target population of marginalized residents may comprise the following:

- Persons with disabilities
- Migrants;
- Homeless persons;
- Destitute;
- Drug Addicts,
- Domestic Workers;
- Prisoners, including Juvenile delinquents in institutions;
- Patients suffering from diseases like, leprosy that results in isolation from society;
- Widows/ Aged Residents/senior citizen and;
- Such vulnerable groups like Sex-workers/transgender.

For governments and individuals alike, strong identity for residents has real economic value. While weak identity systems cause the individual to miss out on benefits and services, it also makes it difficult for the government to account for money and resource flows across a country. In addition, it complicates government efforts to account for residents during emergencies and security threats.

I&A mechanisms may be classified into three categories as “what you know”, “what you have”, and “who you are”. Each authentication factor covers a range of elements used to authenticate or verify a person’s identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

Ownership factors: Something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone)

Knowledge factors: Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question))

Inherence factors: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

I&A mechanisms should be selected based on the security needs of a service.

6.3 Role of Biometrics in I&A of Citizens

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. Biometric technologies are thus defined as the “automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioural characteristic”. A biometric system can be either an identification system or a verification (authentication) system which are defined below.

Identification - One to Many: A one-to-many comparison of an individual's submitted biometric sample against the entire database of biometric reference templates to determine whether it matches any of the templates.

Verification - One to One: A comparison of two sets of biometrics to determine if they are from the same individual.

Biometric authentication requires to compare a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (*Capture, Process, Enroll*) followed by a *Verification* or *Identification*.

During *Capture*, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera, distinguishing characteristics are extracted from the raw biometric sample and converted into a processed biometric identifier record (biometric template). Next is the enrolment in which the processed sample (a mathematical representation of the template) is stored/registered in a storage medium for comparison during authentication. In many commercial applications only the processed biometric sample is stored. The original biometric sample cannot be reconstructed from this identifier.

6.3.1 Biometric Characteristics

There are many biometric characteristics [35, 59, 60, 78] that may be captured in the first phase of processing. However automated capturing and automated comparison with previously stored data requires the following properties of biometric characteristics:

- *Universal*. Everyone must have the attribute. The attribute must be one that is universal and seldom lost to accident or disease.

- *Invariance of properties.* They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.
- *Measurability.* The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.
- *Singularity.* Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye colour are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.
- *Acceptance.* The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.
- *Reducibility.* The captured data should be capable of being reduced to a file which is easy to handle
- *Reliability and Tamper-resistant.* The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.
- *Privacy.* The process should not violate the privacy of the person.
- *Comparable.* Should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.
- *Inimitable.* The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

Among the various biometric features, those being considered for I&A in e-Governance applications are fingerprint, facial features, iris, signature etc.

Fingerprint

Fingerprint biometric is an automated digital version of the old ink-and-paper method used for more than a century for identification, primarily by law enforcement agencies. The biometric device involves each user to place his finger on a platen for the print to be read. Fingerprint biometrics currently has three main application arenas: large-scale Automated Finger Imaging Systems (AFIS) generally used for law enforcement purposes, fraud prevention in entitlement programs, physical and computer access. A major advantage of finger imaging is the long-time use of fingerprint and its wide acceptance by the public and law enforcement communities as a reliable means of human recognition. Others include the

need for physical contact with the optical scanner, possibility of poor quality images due to residue on the finger such as dirt and body oils (which can build up on the glass plate), as well as eroded fingerprints from scrapes, years of heavy labour, or mutilation.

Facial Recognition

Face recognition [83] is a non-invasive process where a portion of the subject's face is photographed and the resulting image is reduced to a digital code. Facial recognition records the spatial geometry of distinguishing features of the face. Facial recognition technologies can encounter performance problems stemming from such factors as non-cooperative behaviour of the user, lighting, and other environmental variables. The main disadvantages of face recognition are similar to problems of photographs. People who look alike can fool the scanners. There are many ways in which people can significantly alter their appearance like slight change in facial hair and style.

Iris Scan

Iris scanning measures the iris pattern in coloured part of the eye, although iris colour has nothing to do with the biometric [33, 34]. Iris patterns are formed randomly. As a result, the iris patterns in the left and right eyes are different, and so are the iris patterns of identical twins. Iris scan templates are typically around 256 bytes. Iris scanning can be used quickly for both identification and verification applications because of its large number of degrees of freedom. Disadvantages of iris recognition include problems of user acceptance, relative expense of system as compared to other biometric technologies and the relatively memory intensive storage requirements.

6.3.2 Problems of Using Biometric Identification

Different technologies may be appropriate for different applications, depending on perceived user profiles, need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters. Biometrics has also some drawbacks and loop holes, so there are some problems in using the biometrics system. Some of the well known problems are as follows:

- *The Level of Public Concern about Privacy and Security is Still High*

The privacy issues are defined as the freedom from the unauthorized intrusion. Three distinct forms in which it can be divided are:

- Physical privacy or the freedom of individual from contact with other.

- Informational privacy or the freedom of individual to limit accessing to certain personal information about oneself.
- Decision privacy or the freedom of individual to make private choices about the personal and intimate matters.

Public resistances to these issues can be a big deterrent to a widespread use of biometric-based identification.

Table 6.1: Properties of Biometric Factors

Characteristic	Fingerprints	Face	Iris	Signature
Ease of Use	High	Medium	Medium	High
Error incidence	Dryness, dirt, age	Lighting, age, glasses, hair	Poor Lighting	Changing signatures
Accuracy	High	High	Very High	High
User acceptance	Medium	Medium	Medium	Medium
Required security level	High	Medium	Very High	Medium
Long-term stability	High	Medium	High	Medium

- *Biometric Technologies Do Not Fit Well in Remote Systems*

If the verification takes place across a network (the measurement point and the access control decision point are not co-located), the system might be insecure. In this case, attacker can either steal the person's scanned characteristic and use it during other transactions or inject his characteristic into the communication channel. This problem can be overcome by the use of a secure channel between the two points.

- *Biometric Systems Do Not Handle Failure Well*

If someone steals one's template, it remains stolen for life. Since it is not a digital certificate, or a password, you cannot ask to the bank or to some trusted third party to issue a new one. Once the template is stolen, it is not possible to go back to a secure situation.

6.4 Unique ID Card System as vehicle for Biometric I&A

The Unique Identification Authority of India (UIDAI) has been created with the mandate of providing a Unique Identity (Aadhaar) to all residents of India. With the Aadhaar enrolment already taking place at many locations across the country, the downstream services and applications of the Unique Identification (Aadhaar) number shall need to be formulated and

operationalized. The UIDAI proposes to provide online authentication using demographic and biometric data. It has been given the task of putting in place a mechanism to issue Indian residents with a unique number (UID) which can be used with ease to establish identity and can be verified and authenticated in an easy, cost-effective way to eliminate fraud and duplicate identities.

The purpose of Authentication is to enable Aadhaar-holders to prove identity and for service providers to confirm the resident's identity claim in order to supply services and give access to benefits. Aadhaar Authentication shall make life simpler to the resident as it is meant to be a convenient system to prove one's identity without having to provide identity proof documents whenever a resident seeks a service.

Aadhaar Authentication [72, 73, 74, 75] is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data is submitted to the Central Identities Data Repository (CIDR) for verification, following which the CIDR verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it. The UIDAI confirms either proof of identity or verifies the information provided by the resident based on the data available in the CIDR at the time of Authentication. To protect resident's privacy, Aadhaar authentication service responds only with a "yes/no" and no Personal Identity Information (PII) is returned as part of the response.

The "Aadhaar Authentication Framework" [72] details the Authentication types offered by UIDAI. Aadhaar authentication provides several ways in which a resident can authenticate themselves using the system. At a high level, authentication can be 'Demographic Matching and/or 'Biometric/ OTP Matching. But, in all forms of authentication the Aadhaar Number needs to be submitted so that this operation is reduced to a 1:1 match.

Aadhaar Authentication is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data is submitted to the Central Identities Data Repository (CIDR) for matching following which the CIDR verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it.

Authentication shall enable residents to prove their identity based on the demographic and/ or biometric information captured during enrolment, thus making the process of identification convenient and accurate. Aadhaar Authentication shall make life simpler for residents and eliminate the distress and inconvenience in establishing their identity for availing services. Through Aadhaar Authentication, more residents shall be able to prove their identity and

thereby become eligible to benefit from Government schemes and subsidies. Aadhaar Authentication shall help Authentication User Agencies (AUAs) in delivering services to eligible beneficiaries based on establishing their identity, thus improving efficiency and transparency in service delivery to the common man.

Authentication Service Agencies (ASAs) can offer AUAs multiple protocols and options for connecting their solution to Aadhaar system and in addition provide reporting and other value added services. If ASA is a telecom provider, then a full connectivity solution could be provided to an AUA for end to end Aadhaar authentication. At a basic level, ASA service is that of forwarding API calls from AUAs to CIDR through a secure connection. ASA server should be built like a middleware or enterprise service bus that allows secure incoming connections from AUAs to be verified, audited, and then invoking API URLs exposed by Aadhaar servers through HTTPS and then sending the response back to AUAs. A complete ASA server could be thought of as a middleware (or Enterprise Service Bus – ESB) providing multiple protocol support, multiple data format support, with built-in format translation and other capabilities such as auditing and reporting.

ASA server could be as simple as an HTTP proxy, where as a more advanced ASA server could allow multiple incoming protocols from AUAs there by providing more options to AUAs. For example, in addition to HTTPS as a synchronous protocol, ASA server could allow AUAs to use asynchronous schemes using a messaging interface. Figure 6.1 depicts a high level architecture of an ASA server.

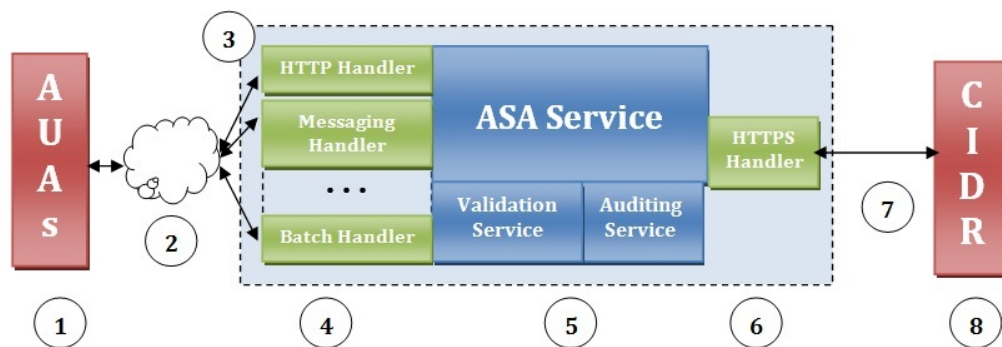


Figure 6.1: ASA Server Architecture

Aadhaar is a permanent and non-revocable identity as opposed to currently existing identity systems which are based on local, revocable credentials. Hence, AUAs are encouraged to use Aadhaar Authentication in conjunction with the AUA's existing authentication process so as to strengthen their authentication process. Aadhaar Authentication should be perceived as a mechanism to strengthen the current authentication process followed by AUAs to authenticate

residents/ beneficiaries and enhance the level of identity authentication assurance while providing convenience to the resident.

It should be noted that the Aadhaar authentication system is not a 100 percent accurate system, irrespective of the kind of attributes selected for authentication. In cases where Authentication Device operator has sufficient reason to conclude that the outcome of an Aadhaar authentication result is not accurate, the operator may explore alternate mechanisms, including verification of Proof of Identity/ Proof of Address documents for establishing the identity of a genuine resident. The AUA shall put in place practices and procedures for handling exceptions so as to deliver services to all genuine beneficiaries.

Aadhaar Authentication supports:

1. Demographic Matching
2. Biometric Matching and
3. Additional features such as One-Time-Password (OTP)

6.4.1 Demographic Matching

Demographic matching refers to the usage of Aadhaar Authentication system by AUAs for matching Aadhaar number and the demographic attributes (name, address, date of birth, gender, etc. as per API specifications) of a resident in the CIDR with the data in the AUA's database or with demographic data submitted at the point of authentication.

For example, demographic matching could be used by:

- Banks for automated Know Your Customer (KYC) checking
- Any government welfare scheme for eliminating fake and duplicate identities in their databases
- Telecom service providers for address verification
- Private institutions/ banks for date of birth verification

6.4.2 Biometric Matching

Biometric Matching refers to the usage of Aadhaar Authentication for matching the biometric attributes of a resident in the CIDR to the biometric data submitted by the resident on an authentication device.

For example, biometric matching could be used by:

- Banks for establishing identity of customers before starting a new bank account

- Telecom service providers before issuing a new mobile connection
- Any organization for attendance tracking

6.4.3 Matching using any other factors such as One-Time-Password (OTP)

In this case, an OTP is sent to the registered mobile phone number of the resident seeking Aadhaar Authentication. The OTP shall have a limited validity. The resident shall provide this OTP during authentication and the same shall be matched with the OTP at the CIDR.

For example: OTP based authentication could be used by

- Banks for authenticating customers during internet banking transaction
- E-commerce companies before completing a cash-on-delivery transaction

6.4.4 Uses of Aadhaar Authentication

The authentication service provided by UIDAI can be used by the AUA or the Sub AUA for the following purposes:

1. Establishing Identity during Know Your Citizen (KYC) or during service delivery

Biometric confirmation to add new users / customers – Aadhaar is envisaged to provide identity to the unreached & marginalized. Aadhaar-based biometric authentication would allow such residents access to critical services such as banking & telecom. This usage will also help manage cases of impersonation / false identity in services such as obtaining new phone connection, credit cards etc. Various financial institutions like banks could use Aadhaar authentication to establish the identity of customers before starting a bank account for new customers through biometric matching. Similarly, telecom service providers could use Aadhaar authentication to authenticate customers and establish their real identity, before issuing new connections (SIM cards) and duplicate SIM cards.

Confirming Beneficiary – Various social sector programs where beneficiaries need to be confirmed before delivery of the service are expected to be the most common users of the authentication service. Examples of some such usages include food grain delivery to PDS beneficiaries, health service delivery to Rashtriya Swastha Bima Yojna (RSBY) beneficiaries, registering job applications by National Rural Employment Guarantee Act (NREGA) beneficiaries etc. This usage would ensure that services are delivered to the right beneficiaries.

Attendance tracking – Another key usage of authentication would be attendance tracking for programs such as Sarva Shiksha Abhiyan (SSA) (for students & teachers), NREGA where wages / outlay is linked to actual number of days the beneficiary reports for the program etc.

Financial transactions – One of the biggest benefits of Aadhaar-based authentication is expected to be in financial inclusion segment. Micro-ATM devices on Aadhaar-based authentication have the potential of changing financial landscape of the country. Various internet, social networking and e-commerce related websites could also use Aadhaar Authentication to authenticate customers/ subscribers whenever it is required to establish the real identity of the person who subscribes or does a transaction. Besides standard security related requirements such as entry to airports, hotels etc., new usages of Aadhaar-based authentication could be as identity proofs in various examinations (such as medical, engineering entrance etc.) where a large number of cases of impersonation are reported every year.

Address verification – Address verification, which is a key requirement for providing some of the services like telephone connection, banking products, could be done through Aadhaar-based authentication. This is expected to substantially reduce the cost of KYC in providing these services & at the same time provide a reliable verification mechanism.

Demographic data verification – Demographic data like date of birth can also be verified through Aadhaar authentication.

2. Elimination of fake and duplicate identities in existing application and database

During enrolment, de-duplication is done (using biometrics) to issue Aadhaar numbers to residents and hence, the Aadhaar numbers are unique. Hence, when Aadhaar numbers are seeded into existing databases, it can help in elimination of fake and duplicate identities, thereby cleansing the database. For e.g. Public Distribution System (PDS) databases can be cleansed of all fake and duplicate identities by seeding Aadhaar number into it, as each person will have only one Aadhaar number.

Once the Aadhaar numbers are seeded into the database, one-time authentication of new beneficiaries/ customers can be done during their enrolment into the respective programs/ schemes and this shall prevent fake and duplicate identities from entering existing databases.

3. Improving efficiency & transparency of service delivery

Track end-to-end service delivery process – At a transaction level, Aadhaar-based authentication if implemented across the service delivery process / supply chain will help curb leakages and diversions, and help identify bottlenecks in delivery. Some such applications would be:

- In PDS, track food grain as it is exchanged between PDS intermediaries
- In NREGA, track job application, job assignment, attendance, muster rolls & wage payments
- Link Janani Suraksha Yojna (JSY), Integrated Child Development Services (ICDS) and SSA to ensure health and education for every child

Move service delivery towards a demand-driven, “portable”, beneficiary led system –Since beneficiaries can authenticate their Aadhaar anywhere, various service delivery processes can be re-engineered to make delivery more flexible & favorable to the beneficiaries. Some such benefits would include:

- PDS beneficiary need not be tied to one fair price shop (FPS) and can withdraw rations anywhere
- Migrants can access their PDS rations after leaving their village
- Children of migrants can continue school education in the new place as well

Strengthen existing accountability / vigilance procedures – Although various service delivery processes have vigilance groups and monitoring systems in place, the government and the public have no means of verifying whether vigilance checks and inspections were carried out, and who is accountable for delays and leakages. Aadhaar-based authentication of the vigilance officers/inspectors/auditors combined with time stamping & GPS tracking can strengthen the vigilance & accountability activities. Some examples of this usage include:

- Audits during food grain movement in the PDS program to control diversions
- Engineer/Gram Rozgar Sewak activities in NREGA
- Social audits in mid-day meal program, NREGA etc.

Access to relevant MIS and empowerment of beneficiary – Since Aadhaar will be able to uniquely identify each beneficiary, they would be able to check their entitlements, timeline by when services will be delivered to them, log grievances related to poor service / denial of

service etc. without depending on any middle-man. The same can be enabled through self-service kiosks (already being piloted by NRGEA), mobile phones, call centers etc.

6.4.5 Aadhaar Authentication Offerings

UIDAI shall provide demographic, biometric and OTP authentication services to AUAs. UIDAI advocates the federated authentication system wherein, AUAs are encouraged to use Aadhaar Authentication in conjunction with AUA's existing authentication system. AUAs or their Sub AUAs can use Aadhaar authentication services on its own or in conjunction with their own authentication system.

The AUA shall assess the convenience and interests of the resident and the risks/ impact/ consequence of inaccurate authentication and decide on the authentication offering required. In cases where the AUA perceives high probability of spoofing instances, the AUA may consider using multi-factor authentication to eliminate occurrence of such instances.

UIDAI offers the following Aadhaar Authentication offerings:

1. Type 1 Authentication
2. Type 2 Authentication
3. Type 3 Authentication
4. Type 4 Authentication
5. Type 5 Authentication

While Type 1 Authentication is based on demographic attributes, Types 2, 3, 4 and 5 provide additional factors such as biometric and/or OTP. The Aadhaar number all by itself shall not be a factor for Authentication. In general, a biometric/ OTP based authentication offers a higher degree of authentication assurance than a demographic authentication system.

Type 1 Authentication

Type 1 Authentication is based on demographic attributes. The AUAs can use Aadhaar Authentication system for matching Aadhaar number and the demographic attributes (name, address, date of birth, etc. as per the API specifications) of a resident in the CIDR with the data in the AUA's database, on a periodic basis to check validity of the credentials or for cleaning up the AUAs database by removing duplicates.

AUAs can also use demographic authentication for authenticating beneficiaries/ customers/ subscribers prior to any transactions.

NOTE: Type 2 to Type 5 described below provide additional “factors” to strengthen the authentication and may have demographics data as part of it.

Type 2 Authentication

UIDAI offers Type 2 Authentication offering, where the AUA shall authenticate residents based on One-Time-Password (OTP)/ Mobile. This offering (single factor authentication) may be used for authenticating residents where deployment of biometric technology is difficult or not practical.

Type 3 Authentication

UIDAI offers Type 3 Authentication offering, where the AUA shall authenticate residents based on either one of the biometric modality (single factor authentication) using Fingerprint or Iris.

Type 4 Authentication

UIDAI offers Type 4 Authentication offering, where the AUA shall authenticate residents based on either one of the biometric modality (Fingerprint or Iris) and OTP/ Mobile. A combination of fingerprint/ Iris and OTP (two factor authentication) shall give a higher degree of authentication assurance.

Table 6.2: Attributes for Aadhaar Authentication

Authentication Offering	Aadhaar Authentication Attributes
Type 1	<u>Authentication Attributes:</u> Any single/ combination of the following attributes can be used 1. Name 2. Address 3. Date of Birth and other demographic attributes, as per the API document
Type 2	1. One-time-password (OTP)/ Mobile Any of the demographic attributes also may be used
Type 3	<u>Authentication Attributes:</u> 1. Either of Fingerprint or Iris Biometrics Any of the demographic attributes also may be used
Type 4	<u>Authentication Attributes:</u> 1. Either of Fingerprint or Iris and 2. OTP/ Mobile Any of the demographic attributes also may be used
Type 5	<u>Authentication Attributes:</u> 1. Fingerprint and 2. IRIS and 3. OTP/ Mobile Any of the demographic attributes also may be used

Type 5 Authentication

UIDAI offers Type 5 Authentication offering, where the AUA shall authenticate residents based on Fingerprint, Iris and OTP. A combination of fingerprint, Iris and OTP/ Mobile (three factor authentication) shall give a higher degree of authentication assurance.

Table 6.2 provides the attributes for each Authentication Offering. The AUA can choose any attribute/ combination of attributes to achieve the assurance level.

The AUA shall assess the business requirement and may opt to choose biometrics as an attribute for authentication only when the requirement is proportionate and appropriate for the use of biometrics. The AUAs are encouraged to follow the federated authentication model and use Aadhaar Authentication in conjunction with domain specific identifiers and identity credentials as extra authentication attributes to strengthen the AUA's authentication process.

6.5 Security Issues of Unique ID Card System

In any identity authentication program it is important to decide what exception rate is acceptable and how to handle the biometric exception cases. There is no particular biometric modality that can be used to authenticate everyone without exception. So like any other technology even biometrics has exceptions. There will always be a set of population who will be temporarily or permanently excluded from a specific biometric system. We can term this set of people as 'outliers'. Therefore Aadhaar authentication system includes an effective approach where it can accommodate these outliers without causing inconvenience, discrimination to the residents and at the same time not compromising on security aspect. The outliers may fall into one of the following categories:

- People with missing biometric characteristic, for example: No iris or no fingers
- People with hard manual labor (like construction, mine workers) having all of their fingers in extremely poor condition with respect to fingerprint quality
- Injured people having cut finger, broken hand.
- People having illness such as cataract problem, burnt fingers
- Extreme environmental conditions with direct sunlight, high humidity and dryness
- Very young (children) and very elderly population having undefined features, soft and wrinkled skin

Biometric exception can be classified under two categories (i) Failure to acquire (FTA), (ii) Failure to use (FTU).

Failure to acquire (FTA) means the failure of a biometric system to capture an image of sufficient quality and extract biometric data. FTA cases will be mostly associated with the temporary outliers. Firstly, it is very critical to understand the reason for FTA. If the environmental set up is the main reason, for example, in case of Iris, if stray illumination sources or bright lighting conditions is causing iris camera not to acquire an iris, then these condition should be eliminated and a resident should be asked to re-submit his/her Iris. In case of fingers, if FTA is due to extremely dry or dirty skin condition, then a resident may be asked to wash his fingers and then reinsert the finger. Sometimes additional advice/instruction or help from an operator can help in generating a reasonable quality biometric (example: for blind people bringing iris handle held close to the eye and guiding resident to align the iris, for people with arthritis, guiding/helping resident to place finger flat on the sensor or selecting an alternate finger).

In some cases alternate biometric modality can also be used, for example use iris if finger fails or vice versa or alternate biometric samples. For example, (i) use middle finger and thumb instead of just index finger for authentication (ii) use right iris instead of left iris.

It is recommended that in FTA cases, a resident should be allowed to provide multiple attempts (say 3 or 4) with a proper assistance before concluding that a biometric cannot be acquired.

Failure to use (FTU) means the conditions where biometric attributes (fingerprint and/or iris) does not exist or all biometrics are of extremely poor quality. FTU cases are associated with the permanent outliers. Manual intervention/ override have to be implemented for Failure to Use (FTU) cases. Intervention should be done by authorized personnel or operator in any of the following modes:

- Demographic verification: The resident's demographic detail can be obtained from CIDR and verified with the demographic details submitted at the Point of Service/ Authentication point.
- OTP based authentication: In case of FTA/ FTU cases, the operator can use OTP for authentication of the resident.
- Document verification and Photo Verification: By verifying valid Proof of Identity/ Proof of Address documents/ valid Photo identity cards, the operator can establish the authenticity of the resident with reasonable accuracy.

In order to avoid security issues, inconvenience to resident and streamlining the process for exception cases (FTU and FTA), it is strongly recommended that the authentication application should have an option to record these cases along with AUA/operator details for better analytics and problem resolution. For the FTA cases, number of manual override attempts should be tracked and only limited number of manual overrides should be allowed per day per terminal to prevent operator malpractice.

In the implementation of the biometric databases for UIDAI project, the following security issues exist:

- Interoperability problem partly caused by lack of good standardized matching algorithms. The availability of a large variety of sensors may make the problem even harder.
- Biometrics readers can often be fooled by “artifacts” and “spoofing”. Liveness detection is related to this.
- Biometrics captures seem to be inherently challenging in terms of “privacy and security” and online databases may pose a huge privacy concern. Also, there should be a mirror database with each primary database.
- Template transaction from end system to centralized system may have points of attack. In UIDAI system sensor level attack is possible.
- Technology adaptation is a challenge and template aging (for example face images of a person at age 18 and then at age 40) is not well thought out. Research has shown that along with face, fingerprint and iris templates also vary with age and may reduce the matching performance if the templates are not updated regularly.

6.6 The Policy Perspective

As discussed in preceding sections, delivery of online services should be secured by applying appropriate controls, including identification and authentication mechanisms for citizens. However, technical controls can only be implemented if such provisions exist in relevant policies that govern online service delivery.

A policy is a statement of overall intention and direction as formally expressed by management of an organization (ISO/IEC 27003). The content of a policy guides actions and decisions concerning the topic of the policy. An organization may have a number of policies; one for each of the activity areas that is important to the organization. Some policies are independent of each other, while other policies have a hierarchical relationship. In the area of security, policies are commonly organized hierarchically. Typically, the organization’s

security policy is the highest level policy. This is supported by a range of more specific policies, including the information security policy and the Information Security Management System policy. In turn the information security policy can be supported by a number of more detailed policies on specific topics related to aspects of information security. For example the information security policy is supported by policies concerning access control, clear desk and clear screen, the use of network services, and the use of cryptographic controls. It is possible that additional layers of policies may be added in some cases. This is shown in Figure 6.2.

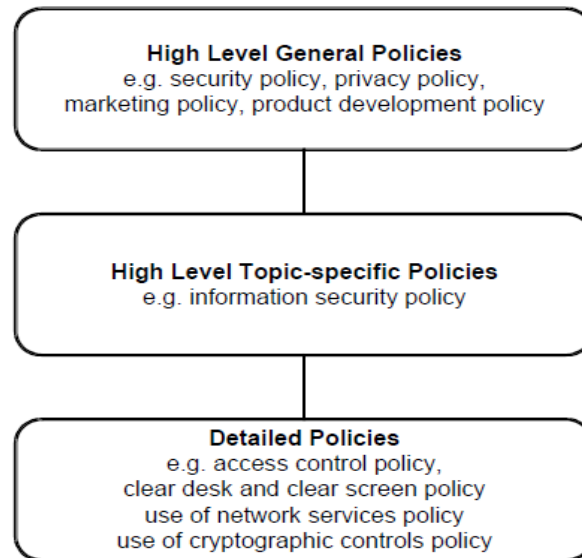


Figure 6.2: Policy Hierarchy

The content of security policies should be based on the context in which a service is delivered. Specifically the following should be considered when developing a policy:

- The aims and objectives of the service
- Strategies adopted to achieve the objectives
- The structure and processes adopted for service delivery
- Aims and objectives associated with the topic of the policy
- The requirements of related higher level policies

Security policies can have the following structure:

- **Policy Summary** – a one or two sentence overview. (This may sometimes be merged with the introduction.)
- **Introduction** – a brief explanation of the topic of the policy.
- **Scope** – describes those parts or activities of an organization that are affected by the policy. If relevant, the scope clause lists other policies that are supported by the policy.

- **Objectives** – describes the intent of the policy.
- **Principles** – describes the rules concerning actions and decisions for achieving the objectives. In some cases it can be useful to identify the key processes associated with the topic of the policy and then the rules for operating the processes.
- **Responsibilities** – describes who is responsible for actions to meet the requirements of the policy. In some cases this may include a description of organizational arrangements as well as the responsibilities of people with designated roles.
- **Key Outcomes** – describes the business outcomes if the objectives are met.
- **Related Policies** – describes other policies relevant to the achievement of the objectives, usually by providing additional detail concerning specific topics.

The following is an example of an information security policy, showing its structure and example content (ISO/IEC 27003).

Information Security Policy (Example)

Policy Summary

Information should always be protected, whatever its form and however it is shared, communicated or stored.

Introduction

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Scope

This policy supports the organization's general security policy. This policy applies to all services provided by the organization.

Information Security Objectives

- Strategic and operational information security risks are understood and treated to be acceptable to the organization.
- The confidentiality of customer information, product development and marketing plans is protected.
- The integrity of accounting records is preserved.

- Public web services and internal networks meet specified availability standards.

Information Security Principles

- All staff and customers will be made aware and accountable for information security.
- Provision will be made for funding information security controls in service delivery processes.
- Possibilities for fraud associated with abuse of information systems will be taken into account in the overall management of information systems.
- Information security status reports will be available.
- Information security risks will be monitored and action taken when changes result in risks that are not acceptable.
- Criteria for risk classification and risk acceptability are found in the ISMS policy.
- Situations that could place the organization in breach of laws and statutory regulations will not be tolerated.

Responsibilities

- The senior management team is responsible for ensuring that information security is adequately addressed for service delivery.
- Each senior manager is responsible for ensuring that the people who work under their control protect information in accordance with the organization's standards.
- The chief security officer advises the senior management team, provides specialist support for the organization's staff, and ensures that information security status reports are available.
- Every staff member has information security responsibilities as part of doing their job.

Key Outcomes

- Information security incidents will not result in serious and unexpected costs or serious disruption of services and business activities.
- Fraud losses will be known and within acceptable bounds.
- Customer acceptance of product or services will not be adversely affected by concerns about information security.

Related Policies

The following detailed policies provide principles and guidance on specific aspects of information security.

- Information Security Management System (ISMS) policy
- Access control policy
- Clear desk and clear screen policy
- Policy concerning mobile code
- Back-up policy
- Policy concerning the exchange of information between organizations
- Policy concerning acceptable use of electronic communications facilities
- Record retention policy
- Policy on the use of network services
- Policy concerning mobile computing and communication
- Policy on the use of cryptographic controls
- Compliance policy
- Data protection and privacy policy

All security policies should support (i) Risk identification, by providing a baseline of controls that can be used to identify gaps in systems designs and implementations, and (ii) Risk treatment, by supporting identification of treatments for identified vulnerabilities and threats. It should also be ensured that these policies comply with the requirements of security standards like ISO/IEC 27001, ISO/IEC 27002, COBIT 5, and relevant laws like Indian IT Act 2000 (amended in 2008) and Information Technology (Electronic Service Delivery) Rules, 2011. Moreover, security policies for online service delivery should address all concerns of citizens, so that G2C services become acceptable and useful.

6.7 Summary

This chapter presented a detailed discussion on the identification and authentication aspects of online service delivery. It has been shown that biometric access control mechanisms supported by Aadhaar cards can be used for I&A of citizens for e-service delivery. The chapter also includes a discussion on the security issues of the Aadhar card system and the policy perspective of online service delivery supported by UIDAI. Special emphasis should be given on addressing concerns of citizens while formulating policies. Besides, policies must adhere to the provisions of relevant security standards, and laws and regulations.

It is recommended that enrolment and registration should be under the supervision of trained and trustworthy staff. Also, there should be a central ID register for public domain

applications to guard against attempts to establish multiple IDs. Finally, the confidentiality, integrity and availability of the ID servers are to be maintained by establishing an ISMS following international standards.

Conclusion and Future Work

7.1 Summary of Contributions

The major contributions of this research are as follows:

1. A brief survey of the inception and development of the concept of governance have been done. This highlights that in India, very rich concept of governance was developed even in the epics and in the writings of Kautilya and others, which are relevant even in the contemporary national and international context.
2. A study on the evolution of the e-Governance models proposed by different agencies, where the commonality of the different models has been brought out. This provides the background of the Chapters to follow.
3. The security requirements of the data in store, data in process, data in transit and data at destination have been analyzed in detail for each of the above models. The access requirements for all the eight types of users for each model have been identified. This enables the structured development of the security of e-Governance institutions. Data security and Access security are considered the two pillars of e-Governance security.
4. The security expectations, security concerns and risk perceptions of the e-Service Delivery Gateways have been identified from the point of view of the stakeholders like citizens, service owners and service suppliers. Based on the identified requirements, the security controls, as per international standards, appropriate for the services delivery gateways have been identified. Security Assurance issues for the gateways have also been addressed.
5. A detailed analysis of the Unique ID Card system has been presented. The security issues related to the Aadhar card system have been identified. A Policy perspective for the Aadhar card system has been introduced.

7.2 Scope of Improvement

There are certain aspects where improvements can be effected in the works which have been done in this dissertation.

In the e-Governance models, the established models of UK and Europe could have enriched the content, though the actual results would have been almost the same.

The security requirements of the e-Governance systems could be enriched by including the threat analysis and effective control selection for the government.

For the service delivery gateways, more emphasis could have been given to the Vulnerability Analysis and Risk Assessment aspects. But this can only be done after they are implemented and in use for some time, so that real-life data can be obtained.

For Aadhar card system, some aspects which have not been touched upon, are the issue of handling such large amount of data, and the issue of registering and providing service to the marginalized section of the society.

7.3 Future Work

Any thesis is not an end by itself. Each thesis raises more questions than it solves. Following are some of the issues identified for future research:

- (a) Mathematical model of the governance system, irrespective of the service delivery technology can be an exciting research topic yielding much needed framework for objective analysis.
- (b) For objective evaluation of the efficiency, efficacy, transparency, robustness, trust and such aspects of e-Governance, such systems can be modeled including the characteristics of the stakeholders, resources and their interrelationships. Of course, the metrics for such properties have to be developed through another relevant research.
- (c) The Risk Analysis and Risk Mitigation aspects can be developed into a mathematical model for objective analysis.

- (d) The Business processes of the service delivery gateways can be identified and their security concerns, control requirements and risks can be computed using the respective mathematical models.
- (e) The issue of Cyber war and Cyber terrorism in the context of e-Governance and e-service delivery are very interesting and contemporary topics of research.
- (f) Finally, the UIDAI system presents a case for detailed research for various issues. The issues of secure and trustworthy collection of biometric data are really concerns which have already been raised from many quarters. The same is true for secure and robust storage and transaction using such data. The privacy aspects of such data will be definitely of concern to the citizens as well as the government.

Though the dissertation has raised and analyzed some issues of concern for the overall e-Governance initiatives of the Govt. of India, the general citizen has already started to enjoy the benefits of these initiatives. It would be reassuring to the governing authorities and other stakeholders to know the issues and the fixes of the IT security of such systems to feel encouraged to use the online services resulting in a prosperous India.

Annexure - I

Timeline of Evolution of Governance

Following is a brief timeline of governance starting from Indus Valley Civilization to Independence of India.

Ancient India Timeline

3000 BC: Beginning of the Indus Valley Civilization

2500 BC: Establishment of the cities of Harappa and Mohenjo-Daro in the Indus Valley

2000 BC: Decline of the Indus Valley Civilization

1600 BC: India is invaded by the Aryans from the west who drive away the Dravidians

1000 BC: One of the earliest Holy Scripture, Rig-Veda is composed

750 BC: Indo-Aryans rule over 16 Mahajanapadas (16 Great States) in northern India, from the Indus to the Ganges

527 BC: Prince Siddhartha Gautama attains enlightenment and becomes the Buddha

327 BC: Alexander the Great of Macedonia invades the Indus valley, fights the famous battle with Porus

304 BC: Magadha king Chandragupta Maurya buys the Indus valley and establishes the Maurya dynasty with Pataliputra as the capital

300BC: Ramayana, a famous epic is composed

220 BC: Maurya dynasty expands to almost all of India

200 BC: Mahabharata, another famous epic is composed

100 BC: Bhagavata Gita is composed

200 AD: The Manu code puts down the rules of everyday life and divides Hindus into four major castes (Brahmins, warriors, farmers/traders, non-Aryans)

390 AD: Chandra Gupta II extends the Gupta kingdom to Gujarat

528 AD: Gupta Empire sees a downfall due to continuous barbaric invasions

550 AD: Chalukyan kingdom is established in central India with capital in Badami

625 AD: Pulikesin extends the Chalukyan Empire in central India

885 AD: Pratihara Empire reaches its peak and extends its empire from Punjab to Gujarat to Central India

997 AD: Mahmud of Ghazni raids northern India

1019 AD: Mahmud Ghazni attacks north India and destroys Kannauj, which is the capital of the Gurjara-Pratihara Empire

Medieval India Timeline

1192 AD: Mohammad of Ghori defeats Prithvi Raj, captures Delhi and establishes a Muslim sultanate at Delhi

1206 AD: The Ghurid prince Qutub-ud-din Aibak becomes the first sultan of Delhi

1490 AD: Guru Nanak Dev Ji establishes Sikhism and the city of Amritsar

1497 AD: Babur, a ruler of Afghan, becomes the ruler of Ferghana and establishes the Mughal dynasty in India

1556 AD: Humayun dies and his son Akbar becomes one of the greatest rulers of India

1611 AD: East India Company is established in India by the British

1627 AD: Shivaji establishes the Maratha kingdom

1707 AD: Aurangzeb dies, destabilizing the Mughal Empire

Modern India Timeline

1751 AD: Britain becomes the leading colonial power in India

1799 AD: British defeat Tipu Sultan

1848 AD: Lord Dalhousie becomes the Governor-General of India

1853 AD: Railway, postal services & telegraph line introduced in India

1857 AD: First War of Indian Independence also known as Revolt of 1857 or Sepoy Mutiny

1858 AD: British Crown officially takes over the Indian Government

1877 AD: Queen of England is proclaimed as the Empress of India

1899 AD: Lord Curzon becomes Governor-General and Viceroy of India

1912 AD: The Imperial capital shifted to Delhi from Calcutta

3rd June 1947 AD: Lord Mountbatten's plan for partition of India comes into light

15th August 1947 AD: Partition of India and Independence from the British rule

Bibliography

- [1] Ackerman, J.: Co-governance for accountability: Beyond “exit” and “voice”. *World Development*. Vol. 32, No. 3, 447-463 (2004)
- [2] Alasem, A.: An Overview of e-Government Metadata Standards and Initiatives based on Dublin Core. *Electronic Journal of e-Government*. 7(1), 1-10 (2009)
- [3] Alawattegama, L., Wattegama, C.: Benchmarking Asia Pacific National Telecom Regulatory Authority Websites. <http://lirneasia.net/projects/2008-2010/indicators-continued/nra-website-survey-asia-pacific-2008/> (2008). Accessed 12 March, 2012
- [4] Apte, V.M.: Political and Legal Institutions. In: *The history and culture of the Indian people*. Vol. 1, The Vedic Age, Majumdar, R.C., Bharatiya Vidya Bhavan Publications (1996)
- [5] Asgarkhani, M.: Strategic Management of Information systems and Technology in an e-World. In: *Proceedings of the 21st IT Conference*. pp103-111, Sri Lanka (2002)
- [6] Asgarkhani, M.: e-Governance in Asia Pacific. In: *Proceedings of the International Conference on Governance in Asia*. Hong Kong (2002)
- [7] Axelsson, K., Melin, f., Lindgren, I.: Developing Public E-Services for Several Stakeholders – A multifaceted view of the needs for an e-service. In: *17th European Conference on Information Systems*. (2009)
- [8] Bagchi, K.: Factors contributing to global digital divide: Some empirical results. *Journal of Global Information Technology Management*. Vol. 8, No. 3, 47-65 (2005)
- [9] Bakos, J.Y.: The emerging role of electronic marketplaces on the internet. *Communications of the ACM*. Vol. 41, No. 8, 35-42 (1998)
- [10] Balasubramanian, N., Corporate Governance in India Traditional and Scriptural Perspectives. In: *The Chartered Secretary*. 385-388 (2005)
- [11] Bannister F.: The curse of the benchmark: an assessment of the validity and value of e-government comparisons. *International Review of Administrative Sciences*. 73 (2), 171-188 (2007)

- [12] Bandopadhyay, S., Sengupta, A., Mazumdar, C.: A quantitative methodology for information security control gap analysis. In: Proceedings of the 2011 International Conference on Communication, Computing & Security (ICCCS 11). India (2011)
- [13] Bokhari, H.: Multi-channel electronic public service delivery mechanisms in developing countries: a case study of the eSahulat programme in Pakistan. In: Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance (ICEGOV). (2010)
- [14] Computer Desktop Encyclopedia: Definition of “e-Services”. Computer Language Company Inc (2010)
- [15] Codagnone, C., Undheim T.A.: Benchmarking eGovernment: tools, theory, and practice. European Journal of ePractice. (2008)
- [16] Dept. of IT, Government of India, “Catalog of Security Controls”, GD 200, 2010.
- [17] DigitalGovernance.org: definition of “Broadcasting / Wider-Dissemination Model”. <http://www.cddc.vt.edu/digitalgov/gov-e-participation-model.html> (2000). Accessed 12 March, 2012
- [18] DigitalGovernance.org: definition of “Comparative Analysis Model”. <http://www.cddc.vt.edu/digitalgov/gov-e-participation-model.html> (2000). Accessed 12 March, 2012
- [19] DigitalGovernance.org: definition of “Critical–Flow Model”. <http://www.cddc.vt.edu/digitalgov/gov-e-participation-model.html> (2000). Accessed 12 March, 2012
- [20] DigitalGovernance.org: definition of “E-Advocacy / Mobilization and Lobbying Model”. <http://www.cddc.vt.edu/digitalgov/gov-e-advocacy-models.html> (2000). Accessed 12 March, 2012
- [21] DigitalGovernance.org: definition of “Interactive-Service Model (G2C2G)”. <http://www.cddc.vt.edu/digitalgov/gov-e-participation-model.html> (2000). Accessed 12 March, 2012
- [22] Ebrahim, Z., Irani, Z.: E-government adoption: architecture and barriers. Business Process Management Journal. Vol. 11, No. 5, 589-611(2005)

- [23] Evans, D., Yen, D.C.: e-Government: evolving relationship of citizens and government, domestic, and international development. *Government Information Quarterly*. Vol. 23, No. 2, 207-235 (2006)
- [24] Evanschitzky, H., Iyer, G.R.: E-Service opportunities and Threats, *Journal of value chain management*, Vol. 1, No. 11(2007)
- [25] Fahnbulleh, N.: The future of electronic government. *Futurics*. Vol. 29, 7-12 (2005)
- [26] Fletcher, P.D.: The government paperwork elimination act: Operating instructions for an electronic government. *International Journal of Public Administration*. Vol. 25, No. 5, 723-736 (2002)
- [27] Forms of Government in Ancient Greek City States: Democracy, Monarchy, Oligarchy, and Tyranny Compared. <http://www.suite101.com/content/forms-of-government-in-ancient-greek-city-states-a84980#ixzzlOryd92WG>(2008). Accessed 12 March, 2012
- [28] Gilbert, D., Balestrini, P., Littleboy, D.:Barriers and benefits in the adoption of e-government. *The International Journal of Public Sector Management*, Vol. 14, 286 – 301 (2004)
- [29] Government of India. Second Administrative Reforms Commission.: Organisational Structure of Government of India. Thirteenth Report, New Delhi, India (2005)
- [30] Government of India. Second Administrative Reforms Commission.: Promting e-Governance: The Smart Way Forward. Eleventh Report, New Delhi, India (2008)
- [31] Graham, S., Aurigi, A.: Virtual Cities, Social Polarisation and the Crisis in Urban Public Space. *Journal of Urban Technology*. Vol. 4, No. 1, 19-52 (1997)
- [32] Gronlund, A., Hatakka, M., Ask, A.:Inclusion in the E-Service Society – Investigating Administrative Literacy Requirements for Using E-Services. In: 6th International Conference (EGOV 2007). Regensburg, Germany (2007)
- [33] Gupta, P., Mehrotra, H., Kaushik, A.K.: Texture-based Iris Recognition System. In: *Proceedings of the SPIE Symposium on Defense and Security Symposium*. Orlando, USA (2008)

- [34] Gupta, P., Mehrotra, H., Rattani, A., Chatterjee, A., Kaushik, A.K.: Iris Recognition using Corner Detection. In: Proceedings of 23rd International Biometric Conference. Montreal, Canada. (2006)
- [35] Gupta, P., Rattani, A., Mehrotra, H., Kaushik, A.K.: Multimodal Biometrics System for Efficient Human Recognition. In: Proceedings of SPIE 'Defense and security symposium. Florida, USA (2006)
- [36] Hai, J.C.: Fundamental of Development Administration. Scholar Press, Selangor (2007)
- [37] Haque, M.S.: E - governance in India: its impacts on relations among citizens, politicians and public servants. International Review of Administrative Sciences. Vol. 68, 231-250 (2002)
- [38] Hassan, M.K., Lu, H., Lu, J.: A framework for delivering personalized e-government services from a citizen-centric approach. In: Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services (iiWAS). (2009)
- [39] Hosey, J., Gamble, R.: Extracting security control requirements. In: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW 10). (2010)
- [40] Helbig, N., Gil-García, J., Ferro, E.: Understanding the complexity of electronic government: Implications from the digital divide literature. Government Information Quarterly, Vol. 26, 89–97 (2009)
- [41] Huang, C.J.: Usability of E-Government Web Sites for People with Disabilities. In: Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE Computer Society (2003)
- [42] Indian Computer Emergency Response Team(CERT-In). Department of Information Technology.: Annual Report(2006). <http://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPT>, India
- [43] Indian Computer Emergency Response Team(CERT-In). Department of Information Technology.: Annual Report(2007). <http://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPT>, India

- [44] Indian Computer Emergency Response Team(CERT-In). Department of Information Technology.: Annual Report(2008). <http://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT>, India
- [45] Indian Computer Emergency Response Team(CERT-In). Department of Information Technology.: Annual Report(2009). <http://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT>, India
- [46] Indian Merchants Chamber: Summary on Kautilya's Arthashastra (2004)
- [47] Jaeger, P.T.: Assessing Section 508 compliance on federal e-government Web sites: A multi-method, user-centered evaluation of accessibility for persons with disabilities. *Government Information Quarterly*. Vol. 23, 169–190 (2006)
- [48] Janda, S., Trocchia, P.J., Gwinner, K.: Consumer perceptions of Internet Retail Service Quality. *International Journal of Service Industry Management*. Vol. 13, No. 5, 412-431 (2002)
- [49] Jiang, J.J., Klein, G., Crampton, S.M.: A note on SERVQUAL reliability and validity in information system service quality measurement. *Decision Sciences*. Vol. 31, No. 3, 725-744 (2000)
- [50] Kane, P.V.: *History of Dharmasastra: Ancient and Mediaeval, Religious, and Civil Law*. Bhandarkar Oriental Research Institute (1975)
- [51] Kaushik, A.K., Mazumdar, C., Bhattacharjee, J., Saha S.: Model-driven Security Analysis of E-Governance Systems. In: *egov India2007 Conference*. New Delhi, India (2007)
- [52] Kaynama, S.A., Black, C.I.: A Proposal to assess the Service Quality of Online Travel Agencies: An Exploratory Study. *Journal of Professional Services Marketing*. Vol. 21, No. 1, 63-88 (2000)
- [53] Kaylor, C., Deshazo, R., Eck, D.V.: Gauging e-government: A report on implementing services among American cities. *Government Information Quarterly (GIQ)*. 18(4), 293 – 307 (2001)
- [54] Lu, J.: Measuring cost/benefits of e-business applications and customer satisfaction. In: *Proceedings of the 2nd International Web Conference*, pp. 139-147. Perth, Australia (2001)

- [55] Mazumdar, C., Kaushik, A.K., Banerjee, P.: On Information Security Issues in e-Governance: Developing Country View. In: egov India2006 Conference. India (2006)
- [56] Moore, C.: The growing trend of government involvement in IT security. In: Proceedings of the 1st annual conference on Information security curriculum development (InfoSecCD). (2004)
- [57] National e-Governance Division: The National e-Governance Plan. http://mit.gov.in/sites/upload_files/dit/files/Compendium_FINAL_Version_220211.pdf, India (2011)
- [58] Ndou, V.: E-Government for developing countries: Opportunities and Challenges. The Electronic Journal on Information Systems in Developing Countries (EJISDC). Vol. 18, No. 1, 1-24 (2004)
- [59] Ngugi, B., Kahn, B.K., Tremaine, M.: Typing Biometrics: Impact of Human Learning on Performance Quality. Journal of Data and Information Quality (JDIQ). Vol. 2, No. 2, 1-21 (2011)
- [60] Overview of Biometric Technologies. In: Encyclopedia of Multimedia Technology and Networking. By Idea Group Reference (2004)
- [61] Pavlichev, A., Garson, G.D.: Digital Government: Principles and Best Practices. IDEA Group Publishing, London (2004)
- [62] Rais, M., Khalid, N.M.: E-Government in Malaysia. Pelanduk Publications, Kuala Lumpur (2003)
- [63] Rowley, J.: An analysis of the e-service literature: towards a research agenda. Internet Research. 16 (3), 339-359 (2006)
- [64] Pomeroy, B.S., Burstein, S.M.: Ancient Greece: Apolitical, Social, and Cultural History. Oxford University Press, New York (1999)
- [65] Schneider, R.M.: A comparison of information security risk analysis in the context of e-government to criminological threat assessment techniques. In: 2010 Information Security Curriculum Development Conference (InfoSecCD 10)
- [66] Shalini, R.: Are Mauritians ready for e-Government services?. Government Information Quarterly. Vol. 26, 536–539 (2009)

- [67] Sharma, S.K., Good Governance in Ancient India. Meerut Journal of Political Science and Public Administration Meerut. Vol. 4, No.1, 109-123 (2003)
- [68] Sheth, J.N., Sharma, A.: E-Services: A framework for growth. Journal of Value Chain Management, Vol.1 (2007)
- [69] Shyam, M., Sunder, S.: Accounting and Governance in Kautilya's Arthasastra. In: The Twelfth World Congress of Accounting Historians at Istanbul. Turkey (2008)
- [70] Smith, S., Jamieson, R., Nguyen, H., Winchester, D.: INFORMATION SYSTEMS SECURITY COMPLIANCE IN E-GOVERNMENT. In: Pacific Asia Conference on Information Systems (PACIS) Proceedings.(2009)
- [71] The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC). 2005. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems - Requirements. Edition 1. Switzerland.
- [72] Unique Identification Authority of India, Govt. of India (GoI): Aadhaar Authentication Framework, Version 1.0, http://uidai.gov.in/images/authDoc/d2_authentication_framework_v1.pdf (2012)
- [73] Unique Identification Authority of India, Govt. of India (GoI): Aadhaar Authentication Implementation Model. Operating Model, Version 1.0, http://uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf (2011)
- [74] Unique Identification Authority of India, Govt. of India (GoI): API Specification Aadhaar Authentication, Version 1.5, http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_5_rev_1_1.pdf (2012)
- [75] Unique Identification Authority of India, Govt. of India (GoI): Role of Biometric Technology in Aadhaar Enrollment, http://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf (2012)
- [76] Valluvar, S.T.: Thiru Kural. English Translation by Subramuniaswami, S.S., Abhinav Publishers, 444 – 448 (2000)
- [77] Vanka, S., Sriram, K., Agarwal, A.: Critical Issues in e-Governance. In: 5th International Conference on e-Governance (ICEG). (2007)

- [78] Vatsa, M., Richa S., Gupta, P., Kaushik, A.K.: Biometric Databases. In: Encyclopedia of Database Technologies and Applications. By Idea Group Reference (2004)
- [79] Wikipedia: definition of “Information and Communication Technology”. http://en.wikipedia.org/wiki/Information_and_communication_technology (2005). Accessed 12 March, 2012
- [80] Wikipedia: definition of “e-Government”. <http://en.wikipedia.org/wiki/E-Government> (2007). Accessed 12 March, 2012
- [81] Wimmer, M., Codagnone, C., Janssen, M.: Future of e-Government Research: 13 research themes identified in the eGovRTD2020 project. In: Proceeding of the 41st Hawaii International Conference on System Sciences, USA (2008)
- [82] Zeithaml, V.A.: Service Excellence in Electronic Channels. Managing Service Quality. Vol. 12, No. 3, 135-139 (2002)
- [83] Zhao, W., Chellappa, R., Phillips, P. J., Rosenfeld, A.: Face recognition: A literature survey. Computing Surveys (CSUR) Journal. Vol. 35, No. 4, 399-458 (2003)